Sentriant Operation Console 2.4 User Guide

Extreme Networks, Inc.
3585 Monroe Street
Santa Clara, California 95051
(888) 257-3000
(408) 579-2800
http://www.extremenetworks.com

Published: July 2007
Part Number: 100212-00 Rev 02

Specifications are subject to change without notice.

Table of Contents

Introduction

Welcome to the *Sentriant Operation Console User Guide*. This user guide gives complete instructions for using the Sentriant Operation Console. Included are user instructions for everyday tasks and administrator instructions for configuring and customizing the Sentriant Operation Console(SOC).

This documentation uses the following conventions:

Menu tabs and subtabs used to access screens are shown in **bold** separated by a greater than symbol. For example instructions for how to get to the Monitoring Sources Panel, which is accessed by first clicking the Monitoring tab, then the Network Topology subtab, and then selecting Sources will be shown as **Setup > Appliance** in the documentation.

Installing Sentriant Operation Console

You must install the Sentriant Operation Console either from the CD that was shipped with your Sentriant Appliance, or by logging in to the Extreme Networks support site and downloading the Sentriant Operation Console software.

To install the Sentriant Operation Console:

Insert the CD and follow the on-screen instructions for installing the Sentriant Operation Console

or

Open a web browser and enter the URL for the Extreme Networks Support site. Follow the instructions for downloading and installing the Sentriant Operation Console.

NOTE

You can download the installer, save it locally and perform the install to reduce network traffic. After downloading, double-click `SOC_x_x_x_xxxx_windows_Installer.exe`.

NOTE

You do not need to install any other software. A Java virtual machine is included with this download.

Follow the on-screen instructions.

Getting Started

Extreme Networks provides an online help system where you can find information for using Sentriant Operation Console.

Running Sentriant Operation Console

To start Sentriant Operation Console in Windows:

Choose **Start** > **Programs** > **Sentriant Operation Console** > **SentriantOpConsole**.

Log In to Sentriant Operation Console

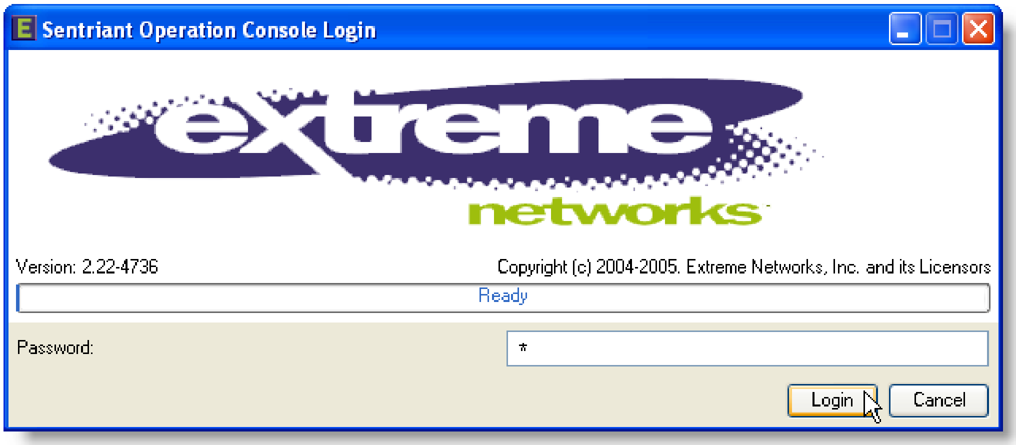
To login to Sentriant Operation Console, you will need to be a user of the system and have the IP Address of a Sentriant appliance which you will be connecting to.

To login to Sentriant Operation Console:

From the Sentriant Operation Console Login screen,

- type in enter your user password

  Example: ******
- Click **Login.**



Sentriant Operation Console Login

Version: 2.22-4736

Copyright (c) 2004-2005. Extreme Networks, Inc. and its Licensors

Ready

Password: *

Using the On-line Help System

Sentriant Operation Console also includes complete documentation in a Java-based help system. The Sentriant Operation Console Help system includes all of the information in this User Guide.

Online Help provides three ways of locating information. The Contents and Index links let you find general information, and the Search link lets you look up specific words or phrases.

To start online Help:

From the File Menu, choose **Help > Sentriant Operation Console Help.**

1 Overview

Welcome to the online Help System for Sentriant Operation Console, a tool for managing multiple Sentriant appliances from one location.

This section provides an overview of the Sentriant Operation Console interface and its tools for locating, organizing, and displaying information. Consult the topics in this section to find out more about the Sentriant Operation Console's Menu Bar, General Status Bar, the Folder List, Information Panel and the Panel Navigation Bar. This section also includes topics on customizing elements of the interface.

To get answers to your questions, use the following tabbed pages in the navigation pane of Sentriant Operation Console Help:

Contents - displays major topics and subtopics. For Windows clients, clicking the plus sign (+) next to the folder icon expands the topic and shows its related subtopics.

Index - displays an alphabetical list of keywords.

Search - displays a box where you can type a term that Sentriant Operation Console Help system will look for in the Help topics.

Glossary - contains definitions for unique terminology used by Sentriant Networks.

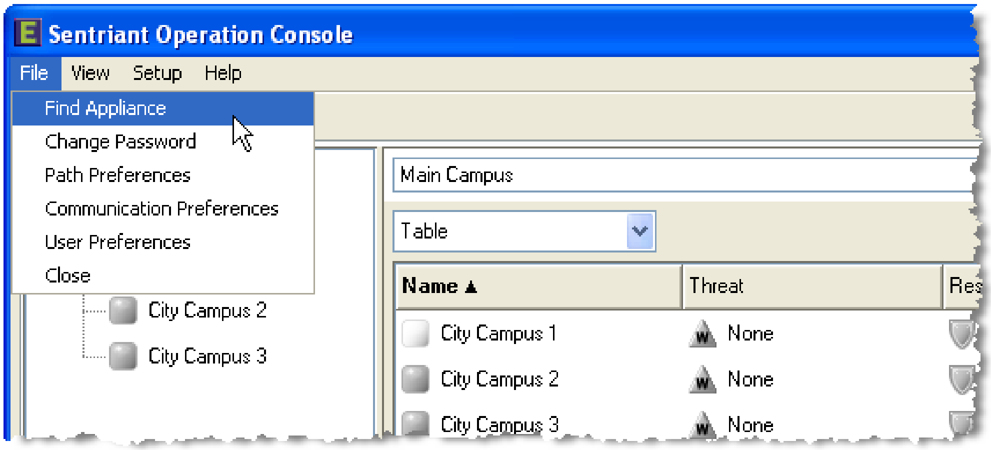
Favorites - gives you quick access to topics that you designate for future reference.

Navigating the Sentriant Operation Console

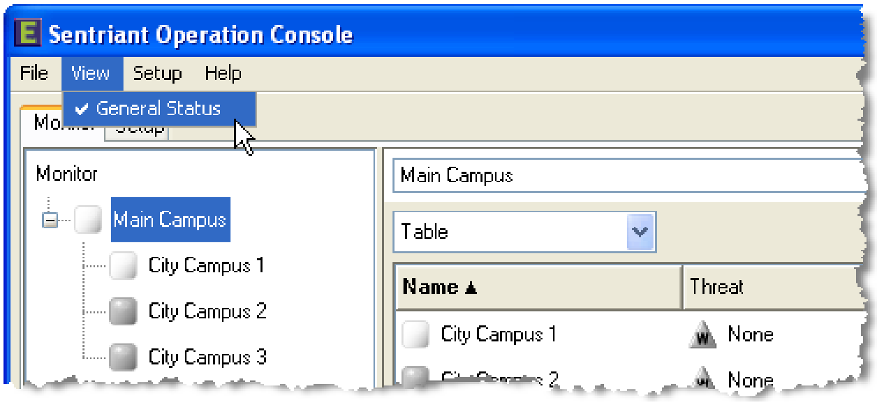
The Sentriant Operation Console provides a variety of standard navigation tools for finding your way around and locating information you need quickly. You can customize views to suit your need or hide them to save space.

Menu Bar

Clicking an item on the Menu Bar opens a drop-down menu of commands. Clicking a menu command either carries out the command or opens a sub-menu or dialog box with additional choices. An arrow symbol next to a command signifies a sub-menu; an ellipsis (...) signifies a dialog box.



Some menu commands turn a view off and on. A check mark next to the menu command indicates that the setting is currently on.

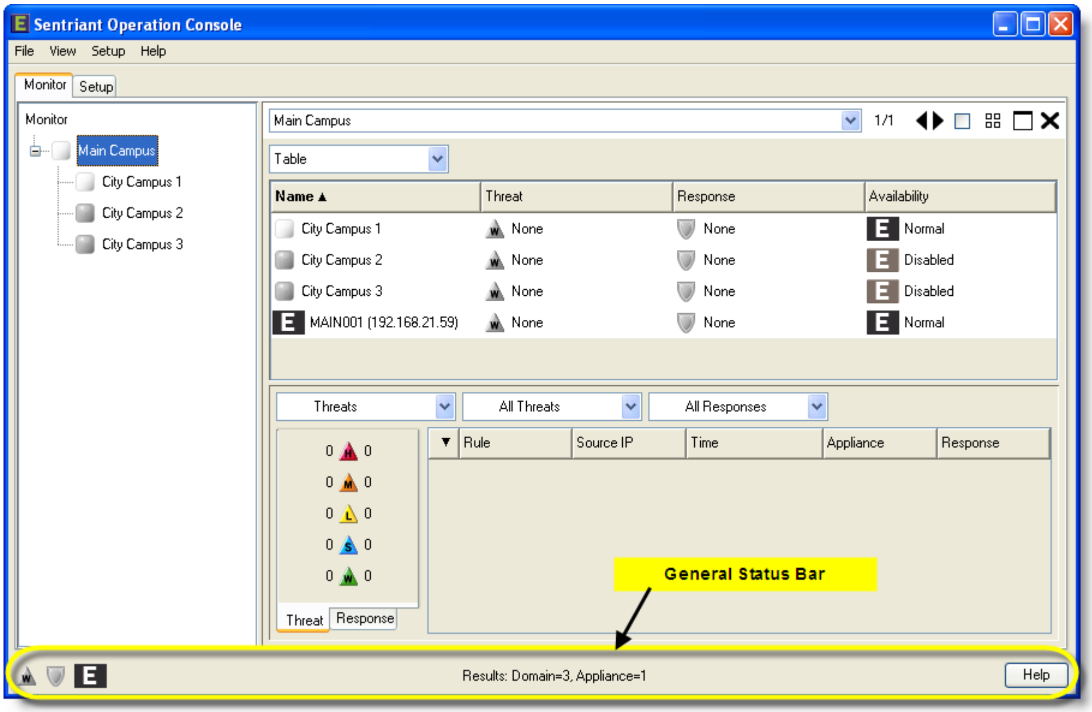


In addition to the pull-down menus on the Menu Bar, shortcut menus are available on certain screens which give you quick access to common commands for a particular context.

Shortcut menus are activated by clicking the right mouse button when the mouse pointer is positioned over an item in a list or in a particular area of the screen. Clicking a command on a shortcut menu will apply to the currently selected list item or the part of the screen where the pointer is resting.

General Status Bar

The General Status Bar displays aggregate sets of threat, response, and health data for all Sentriant appliances managed by the Sentriant Operation Console; a General Status Message containing domain and appliance information, and a button for context-sensitive help.



Name ▲	Threat	Response	Availability
City Campus 1	None	None	Normal
City Campus 2	None	None	Disabled
City Campus 3	None	None	Disabled
MAIN001 (192.168.21.59)	None	None	Normal

	H	
0	H	0
0	M	0
0	L	0
0	S	0
0	W	0

▼	Rule	Source IP	Time	Appliance	Response

Results: Domain=3, Appliance=1

The Threat icons represent an aggregate threat count for all Sentriant appliances managed under SOC. Threat sources that have triggered rules, or that communicate with a target monitored by Sentriant are assigned a priority level. Priority levels are governed by Sentriant appliance policies, rules, and response modes that can be modified or configured as needed to meet network requirements.

The Sentriant appliance supports five priority levels:

H High - the most severe priority level. High priorities take precedence over all other priorities within SOC panels. For example, if a source has triggered a medium and high priority, only the high threat will be shown. A high can be dismissed to a watch.

M Medium - threat rules configured with medium priority take precedence over low, suspect and watches. A medium can be escalated to a high threat or dismissed to a watch.

L Low - threat rules configured with low priority take precedence over suspect and watches. A low can be escalated to a medium or high threat priority or dismissed to a watch.

S Suspect - a source that communicated with a number of unused IP Addresses within a protected segment. A suspect can be escalated to a low, medium, or high threat. Suspect can be dismissed to a watch.

W Watch - a source that communicated within a protected segment. The source may or may not reside within the segment. A watch can be escalated to a suspect, low, medium or high.

The Response icons represent an aggregate threat response for all Sentriant appliances managed under SOC. The detection states are described below:

Cloak - A patent-pending technique by which the Sentriant appliance unilaterally controls and terminates a communications flow between two or more computers.

Deceive, Snare, and Slow Scan - Sentriant appliances use a special ‘deceiving’ technique to engage and hold TCP-based attacks, thus preventing them from spreading. Snaring stops an attacking threat from moving to another computer. Slow Scan send the attacking threat traffic designed to significantly increase the time it takes for an external host to scan the monitored network, causing the attacker to consume time and resources.

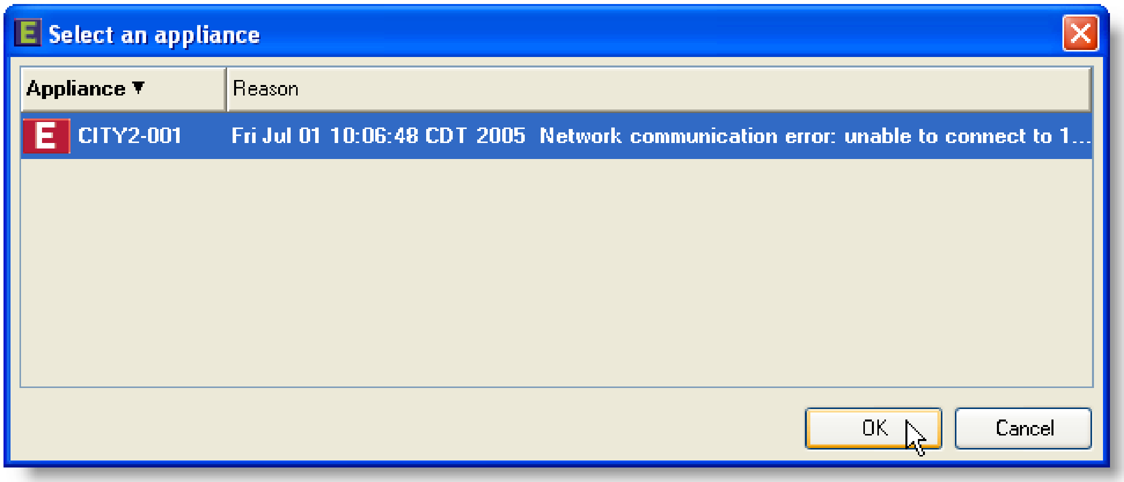
Track - A Sentriant appliance monitors the communication between two or more computers but does not take a response action.

None - No response is invoked.

The Appliance Health icon represent an aggregate operating status for all Sentriant appliance(s) managed under SOC. If an error or warning is encountered with an appliance, the icon will change accordingly displaying the highest severity. For example, a domain made up of four(4) appliances encounters an error with one appliance and another has a warning. The Appliance Health icon will show that there is an appliance with an error since it is a higher severity. Clicking on the icon will navigate to the appliance with the error. The appliance states are described below:

E error	An error has been found with a Sentriant appliance
E warning	A warning with the Sentriant appliance
E normal	The Sentriant appliance is operating normally
E off	The Sentriant appliance is off line

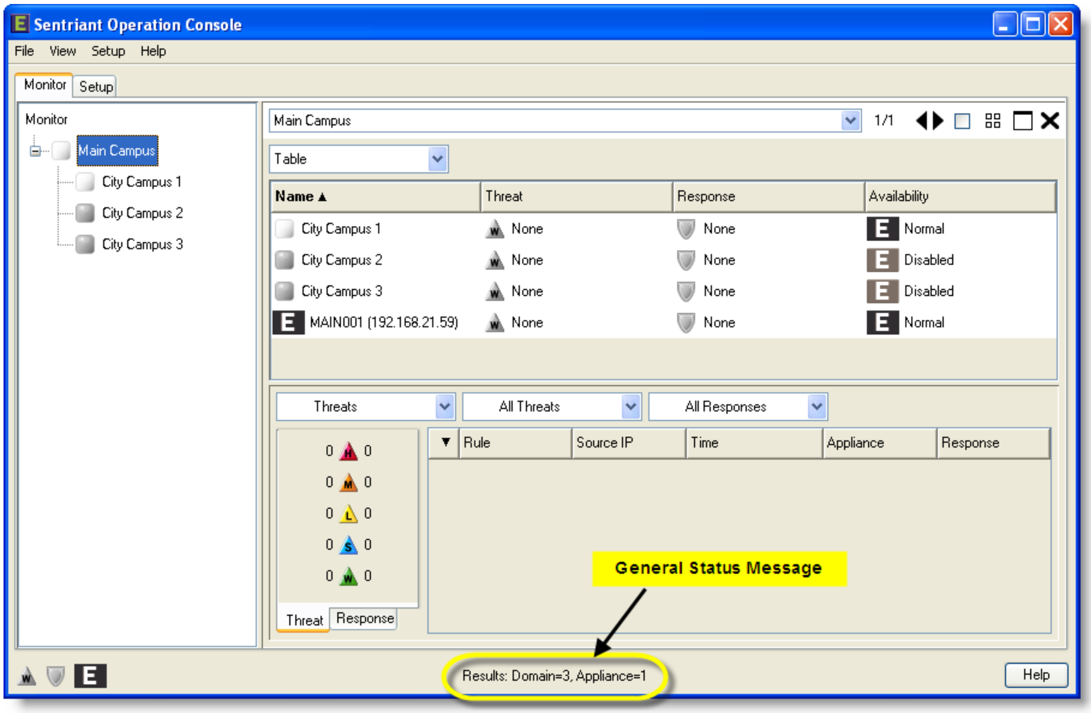
When an appliance is not available, an error message is generated. Clicking on the appliance icon in the General Status Bar opens the Appliance Availability dialog. The message contains a timestamp of when the SOC last tried to contact the appliance, and a message that describes the problem. Selecting the appliance and clicking OK will navigate to the appliance in Setup > Appliance panel.



Select an appliance

Appliance ▼	Reason
E CITY2-001	Fri Jul 01 10:06:48 CDT 2005 Network communication error: unable to connect to 1...

The General Status Message displays a textual representation of the filtering done by the Folder List or Panel Navigation Bar in the Information Panel.



Name ▲	Threat	Response	Availability
City Campus 1	None	None	Normal
City Campus 2	None	None	Disabled
City Campus 3	None	None	Disabled
MAIN001 (192.168.21.59)	None	None	Normal

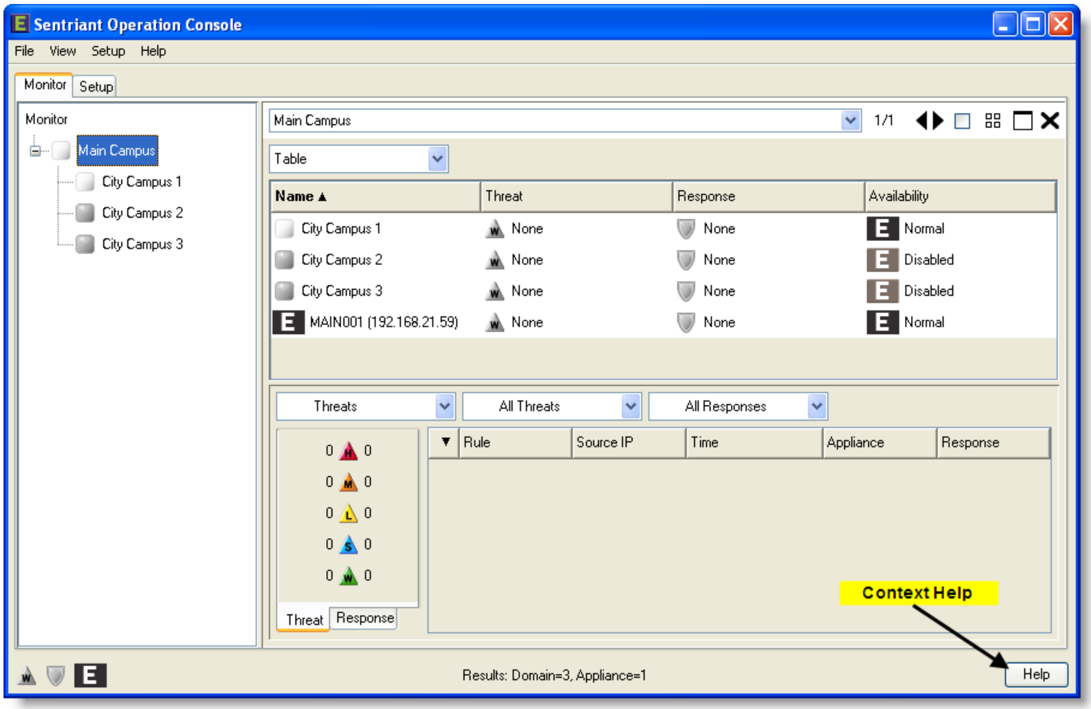
General Status Message

Results: Domain=3, Appliance=1

For example, a query or filter on a domain named Main Campus containing 3 domains and 1 appliance. The General Status Message returns:

Results: Domain=3, Appliances=1.

Clicking the Help button brings up context-sensitive help for the currently displayed panel.



Name ▲	Threat	Response	Availability
City Campus 1	None	None	Normal
City Campus 2	None	None	Disabled
City Campus 3	None	None	Disabled
MAIN001 (192.168.21.59)	None	None	Normal

▼	Rule	Source IP	Time	Appliance	Response

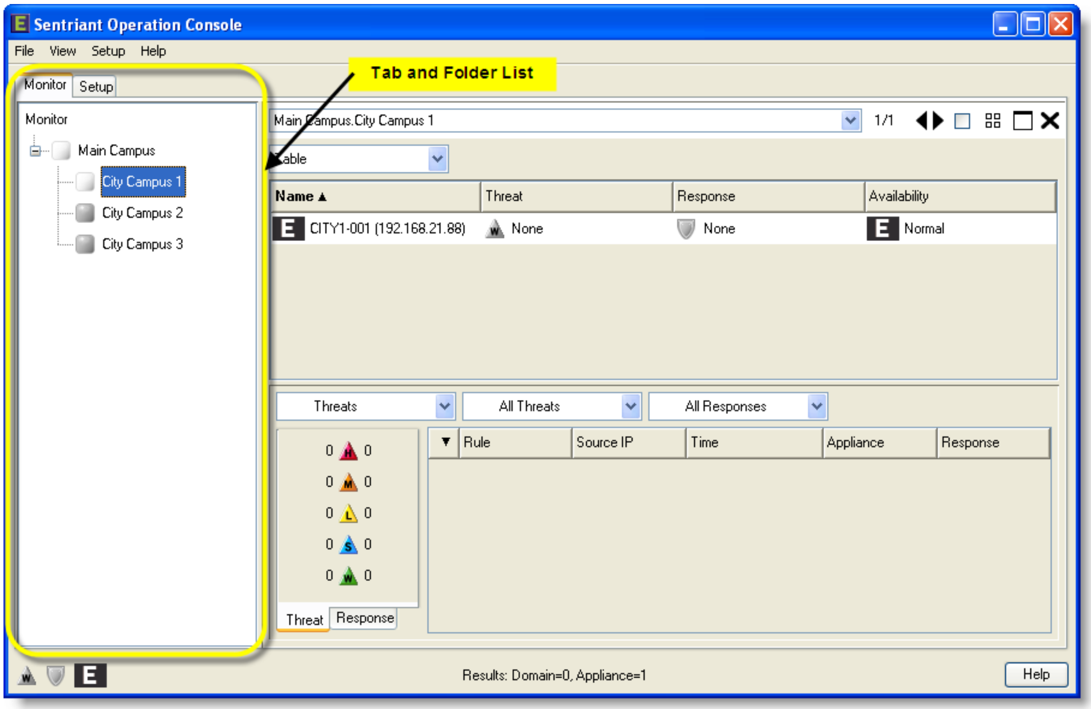
Results: Domain=3, Appliance=1

Tab and Folder List

The main SOC screen is divided into two panels. The left side of the screen is dedicated to navigation and organizing similar information.

The **Tab List** has two tabs, Monitor and Setup. The Monitor Tab contains information and controls to monitor domains and appliances. The Setup Tab contains information and controls to manage SOC configurations of domains, appliances, and policy distributions.

The **Folder List** is a tree list with a hierarchical structure graphically representing domains, appliances and policies managed by SOC. For example, selecting a domain will display the assigned appliance for that domain. For Windows, a plus sign (+) next to a folder icon indicates a closed folder; a minus sign (-) indicates an open folder.



Tab and Folder List

Name ▲	Threat	Response	Availability
CITY1-001 (192.168.21.88)	None	None	Normal

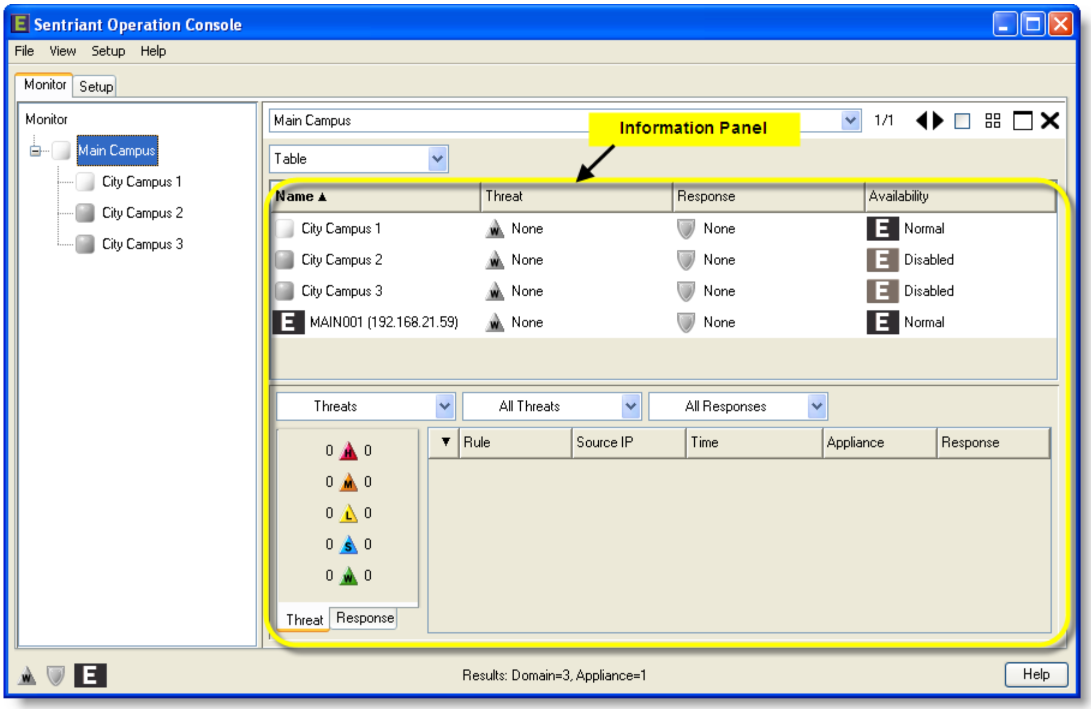
0 H	0
0 M	0
0 L	0
0 S	0
0 W	0

▼	Rule	Source IP	Time	Appliance	Response

Results: Domain=0, Appliance=1

Information Panel

The large area that occupies most of the program window is the **Information Panel** which displays the contents of a selected object. Each object has a corresponding panel that provides menus and tools specific to the tasks that you may need to perform while working in that object.



Information Panel

Name ▲	Threat	Response	Availability
City Campus 1	None	None	Normal
City Campus 2	None	None	Disabled
City Campus 3	None	None	Disabled
MAIN001 (192.168.21.59)	None	None	Normal

0	H	0
0	M	0
0	L	0
0	S	0
0	W	0

▼	Rule	Source IP	Time	Appliance	Response

Results: Domain=3, Appliance=1

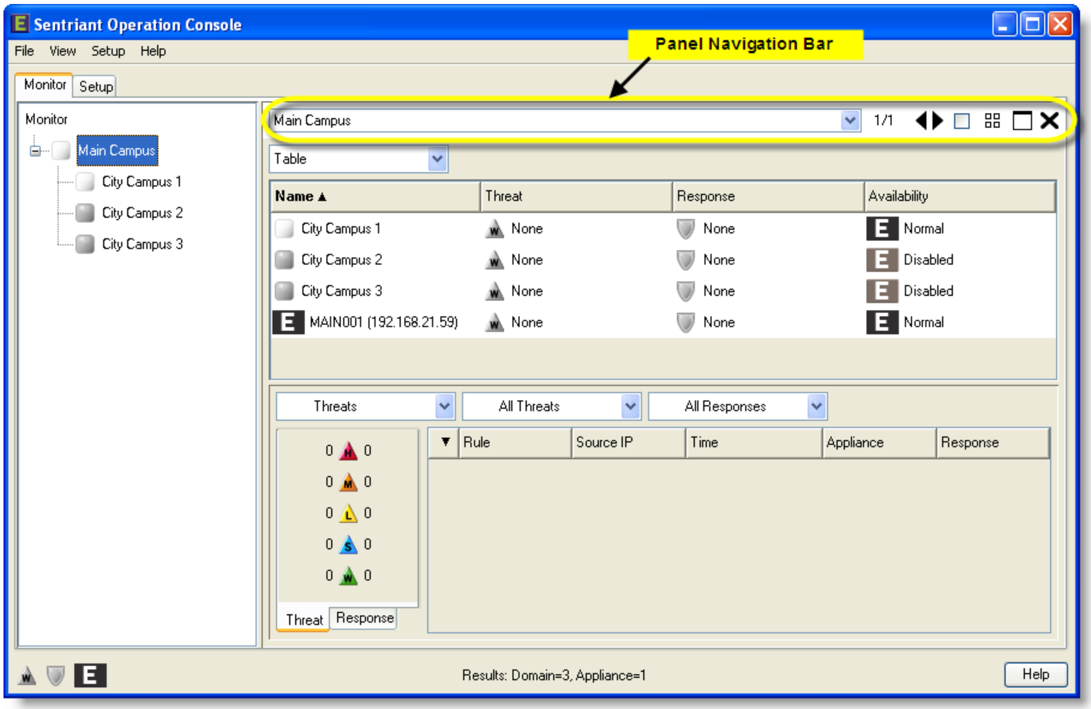
Selecting a tab and then clicking a folder in the Folder List displays one of the following panels:

Monitor - From this panel you can view and manage appliances and threats. The Monitor Panel displays threat and response information rolled up for the selected domain. Selecting an appliance displays only threat and response information for the selected appliance. You may multi-select domains that reside under the main domain and/or appliances to view threat and response information.

Setup - From this panel you can create domains and add appliances as members of SOC. The Setup Panel displays domains and appliances in a navigable tree format. Domains can have multiple layers of domains. Appliance and domains can be moved from one location to another.

Panel Navigation Bar

The Panel Navigation Bar provides a means of changing the way panels are displayed within the Information Panel. A drop down list keeps track of opened category panels. Controls for changing information panels are provided and determine how the panels are displayed. Panels can be turned off, tiled or displayed singularly.



Name ▲	Threat	Response	Availability
City Campus 1	None	None	Normal
City Campus 2	None	None	Disabled
City Campus 3	None	None	Disabled
MAIN001 (192.168.21.59)	None	None	Normal

	H	
0	H	0
0	M	0
0	L	0
0	S	0
0	W	0

▼	Rule	Source IP	Time	Appliance	Response

Results: Domain=3, Appliance=1

Appliance ⌄ Drop down list of opened panels. Selecting a panel from the drop down list will display that panel.

2/3 Indicates the logical ordering of panels under the current top-level node.

◀▶ Click the right or left arrow to scroll forward or backward through the panels.

☑ Keeps the current panel active when you navigate to another panel. When selecting Tile, the panel marked as 'keep' will be displayed in the panel workspace.

⊞ Click the Tile icon to tile all panels that have been opened. The tile panels button is used mainly when you are reviewing charts across multiple segments. By tiling the trend charts, you will see activity across multiple segments on the screen at once.

⧉ Click the icon to maximize or minimize the panel.

✕ Click the icon to close the panel.

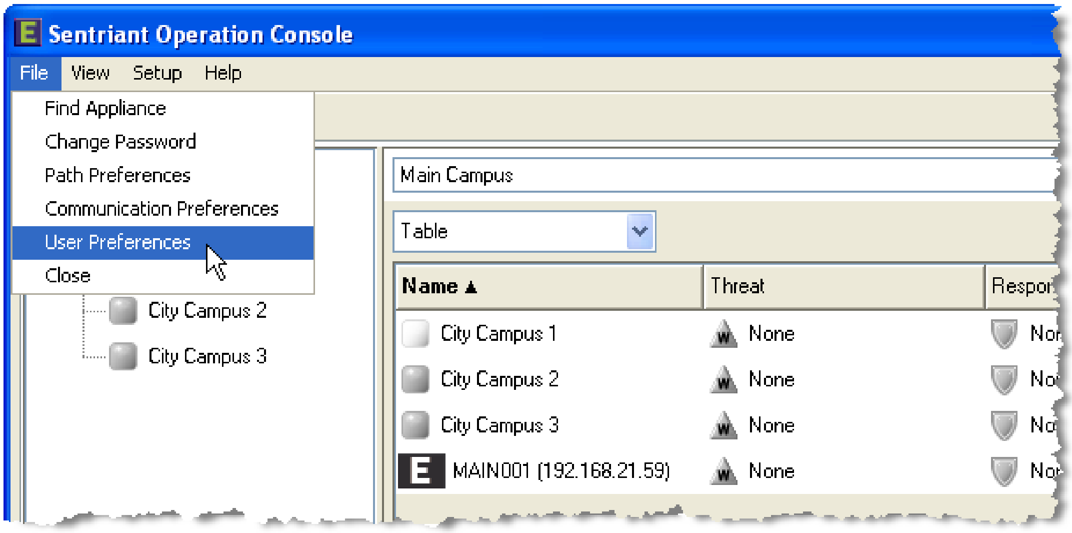
Customizing the Screen

The Sentriant Operation Console displays information in the **Information Panel** as a tabular list of items, along with their major properties. These properties are arranged in columns that you can sort, hide, and resize.

Setting User Preferences

To set user preferences:

1 From the Menu, select **File > User Preferences**.

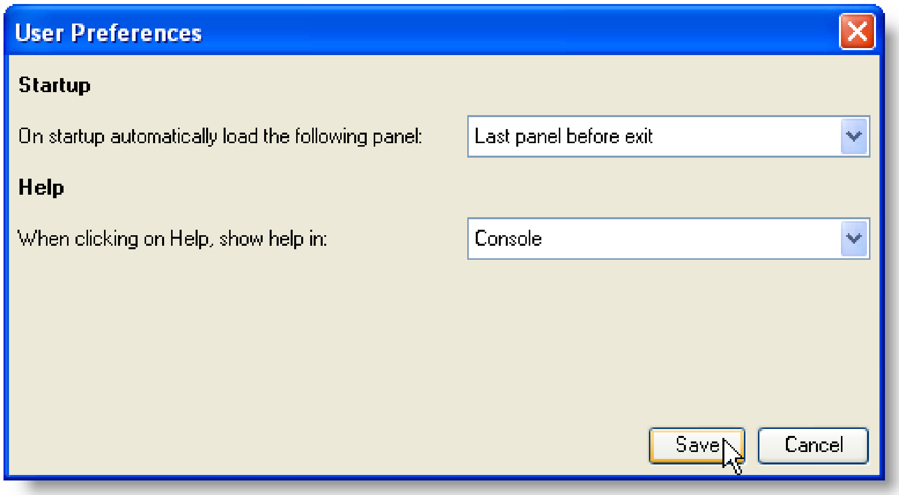


Name ▲	Threat	Respor
City Campus 1	None	Nor
City Campus 2	None	No
City Campus 3	None	No
MAIN001 (192.168.21.59)	None	Nor

The User Preferences dialog opens. From this dialog, you can change the panel that opens when you start SOC and how the help system is displayed.

2 From the Startup drop-down list, select either Last panel before exit or Use current panel. If you select Last panel before exit, the last panel you had open will reopen the next time you start SOC. If you select Use current panel, the panel you have open when setting this option will open the next time you start SOC.

3 From the Help drop-down list, select either Console, Popup Window, or Help System. Selecting Console will display the console with SOC in the information panel, selecting Popup Window will open a browser-like window, selecting Help System will display help in Java Help application.



Startup

On startup automatically load the following panel: Last panel before exit

Help

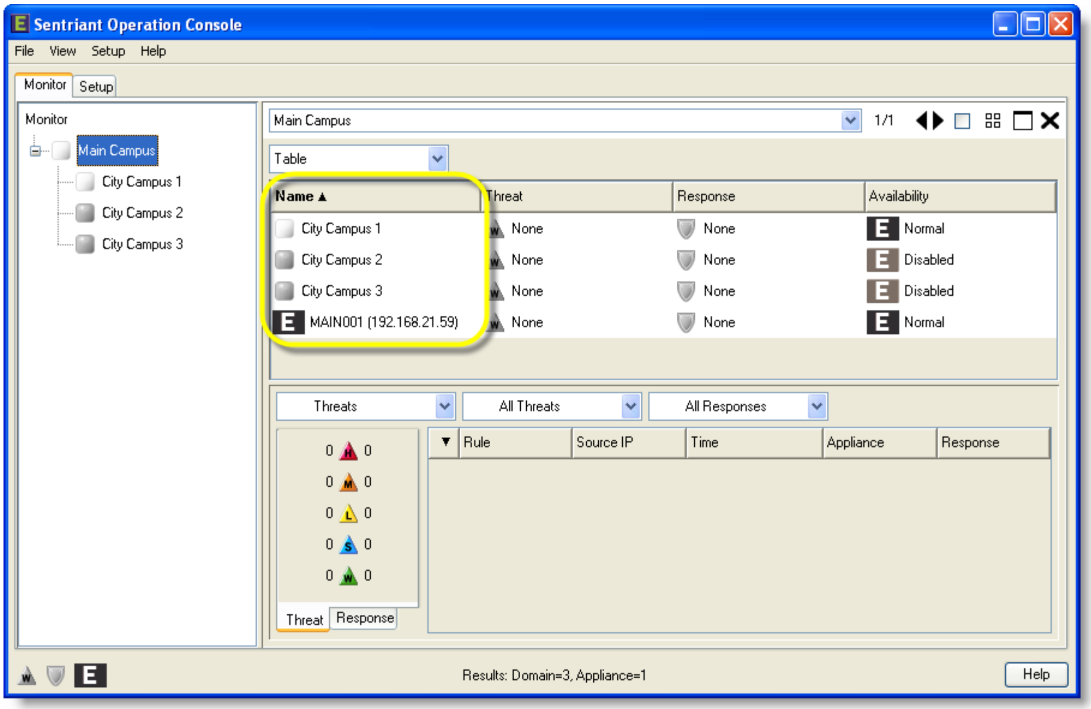
When clicking on Help, show help in: Console

Sorting Data

Sorting arranges data in a list sequentially according to values. Data can either be sorted in an ascending or descending order alphabetically, by threat or response type, availability, and numerically. Clicking a row header in the Information Panel will sort data. See the examples below.

Sorting Alphabetically.

Clicking the Domain row in the Monitor Panel will sort domains alphabetically in an ascending order (A-Z). Clicking again will sort domains in a descending order (Z-A).

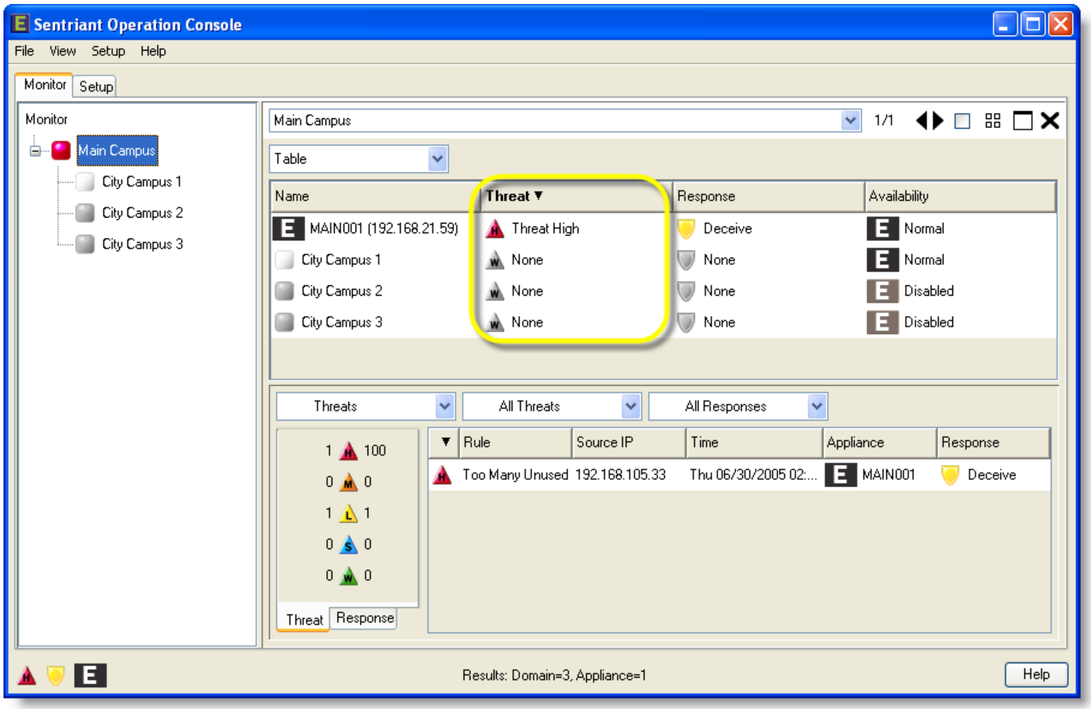


Name ▲	Threat	Response	Availability
City Campus 1	None	None	Normal
City Campus 2	None	None	Disabled
City Campus 3	None	None	Disabled
MAIN001 (192.168.21.59)	None	None	Normal

Results: Domain=3, Appliance=1

Sorting Threats.

Clicking the Threat row header in the Monitor Panel will sort threat detection based on threat priority. When you see the arrow in the row header pointing up, the sort will start with the lowest priority and increase in priority with high at the end of the list. Clicking the row again will sort the list with the highest priority at the beginning of the list and the lowest at the end.



Name	Threat ▼	Response	Availability
MAIN001 (192.168.21.59)	Threat High	Deceive	Normal
City Campus 1	None	None	Normal
City Campus 2	None	None	Disabled
City Campus 3	None	None	Disabled

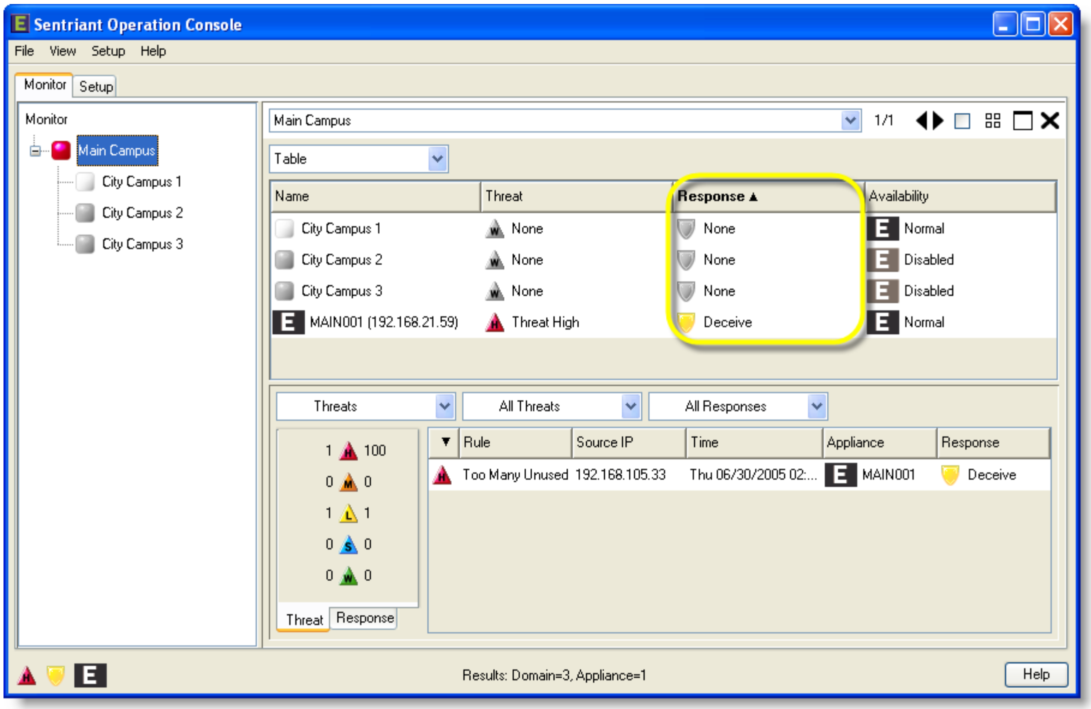
1	H	100
0	M	0
1	L	1
0	S	0
0	W	0

▼	Rule	Source IP	Time	Appliance	Response
	Too Many Unused	192.168.105.33	Thu 06/30/2005 02:...	MAIN001	Deceive

Results: Domain=3, Appliance=1

Sorting Response Type.

Clicking the Response row header in the Monitor Panel will sort responses to threats based on type. When you see the arrow in the row header pointing up, the sort will start with the lowest priority and increase in the following order; None, Track, Deceive/Snare and Cloak at the end of the list. Clicking the row again will sort the list with Cloak at the beginning of the list and None at the end.



Name	Threat	Response ▲	Availability
City Campus 1	None	None	E Normal
City Campus 2	None	None	E Disabled
City Campus 3	None	None	E Disabled
E MAIN001 (192.168.21.59)	Threat High	Deceive	E Normal

1	H	100
0	M	0
1	L	1
0	S	0
0	W	0

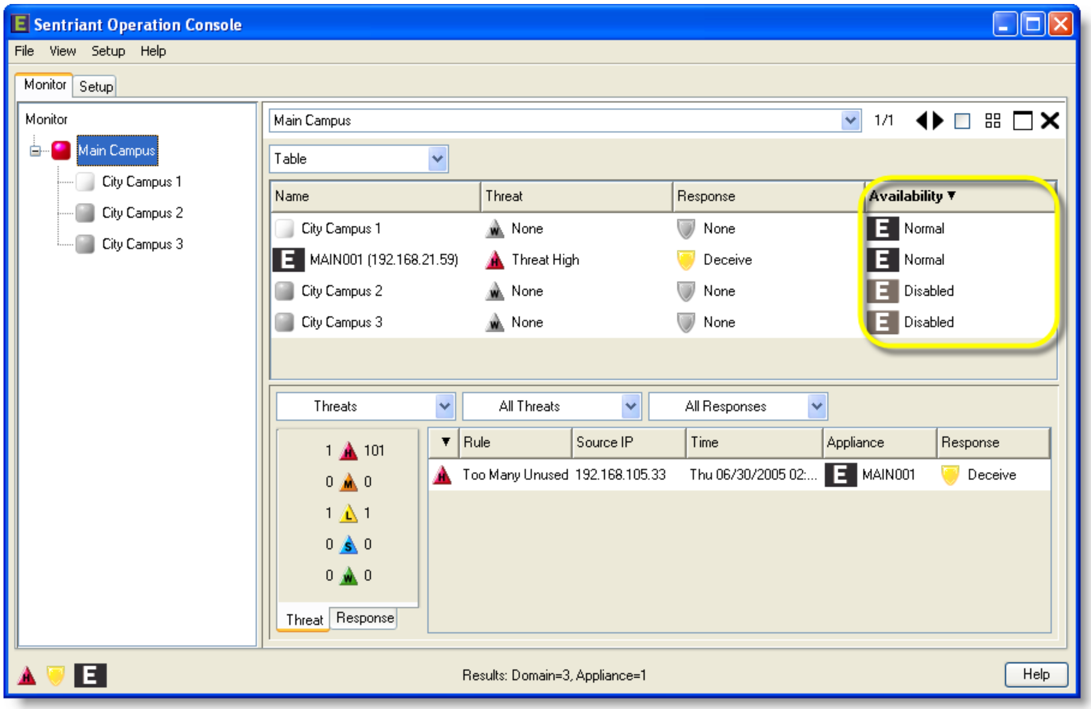
▼	Rule	Source IP	Time	Appliance	Response
H	Too Many Unused	192.168.105.33	Thu 06/30/2005 02:...	E MAIN001	Deceive

Results: Domain=3, Appliance=1

Sorting Availability.

Clicking the Availability row header in the Monitor Panel will sort responses to threats based on appliance health. When you see the arrow in the row header pointing up, the sort will start with the appliances in a normal working state and increase in the following order; Normal, Warning, Error and

Off at the end of the list. Clicking the row again will sort the list with Off at the beginning of the list and Normal at the end.



Name	Threat	Response	Availability ▼
City Campus 1	None	None	E Normal
E MAIN001 (192.168.21.59)	Threat High	Deceive	E Normal
City Campus 2	None	None	E Disabled
City Campus 3	None	None	E Disabled

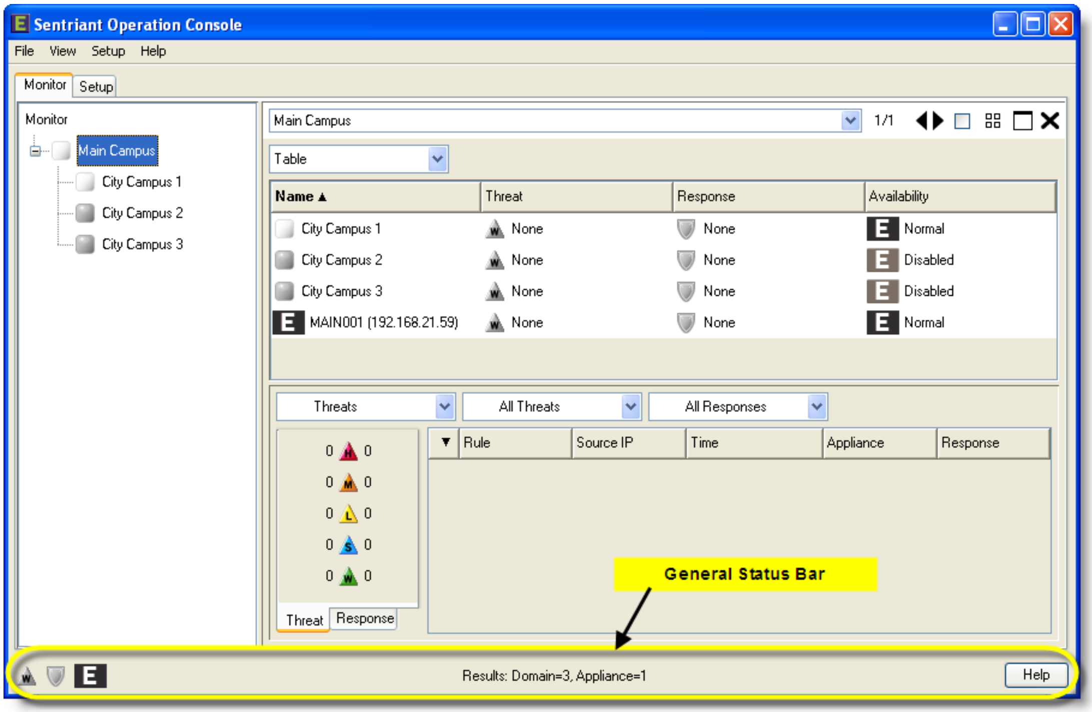
1	H	101
0	M	0
1	L	1
0	S	0
0	W	0

▼	Rule	Source IP	Time	Appliance	Response
H	Too Many Unused	192.168.105.33	Thu 06/30/2005 02:...	E MAIN001	Deceive

Results: Domain=3, Appliance=1

Showing and Hiding General Status Bar

The General Status Bar displays the status of activities for the appliance health, segments, and events. You can hide and show the General Status Bar as needed while you work.



Name ▲	Threat	Response	Availability
City Campus 1	None	None	E Normal
City Campus 2	None	None	E Disabled
City Campus 3	None	None	E Disabled
E MAIN001 (192.168.21.59)	None	None	E Normal

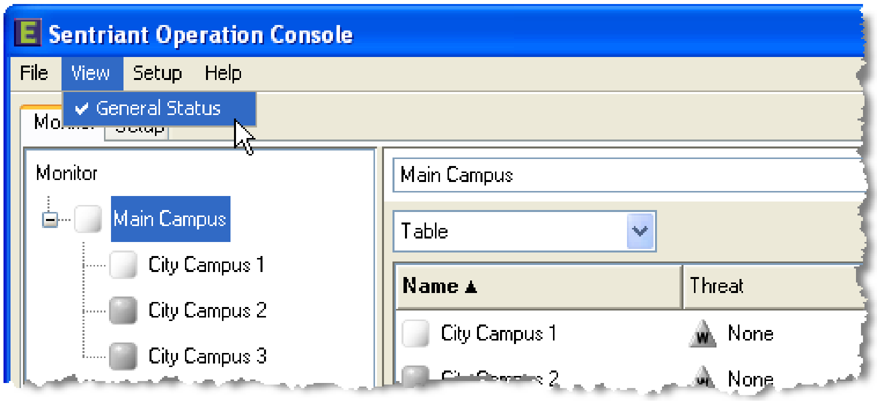
0	H	0
0	M	0
0	L	0
0	S	0
0	W	0

▼	Rule	Source IP	Time	Appliance	Response

Results: Domain=3, Appliance=1

To show or hide the General Status Bar:

From the **View** menu, select **General Status** to hide. A check mark indicates the display is visible.



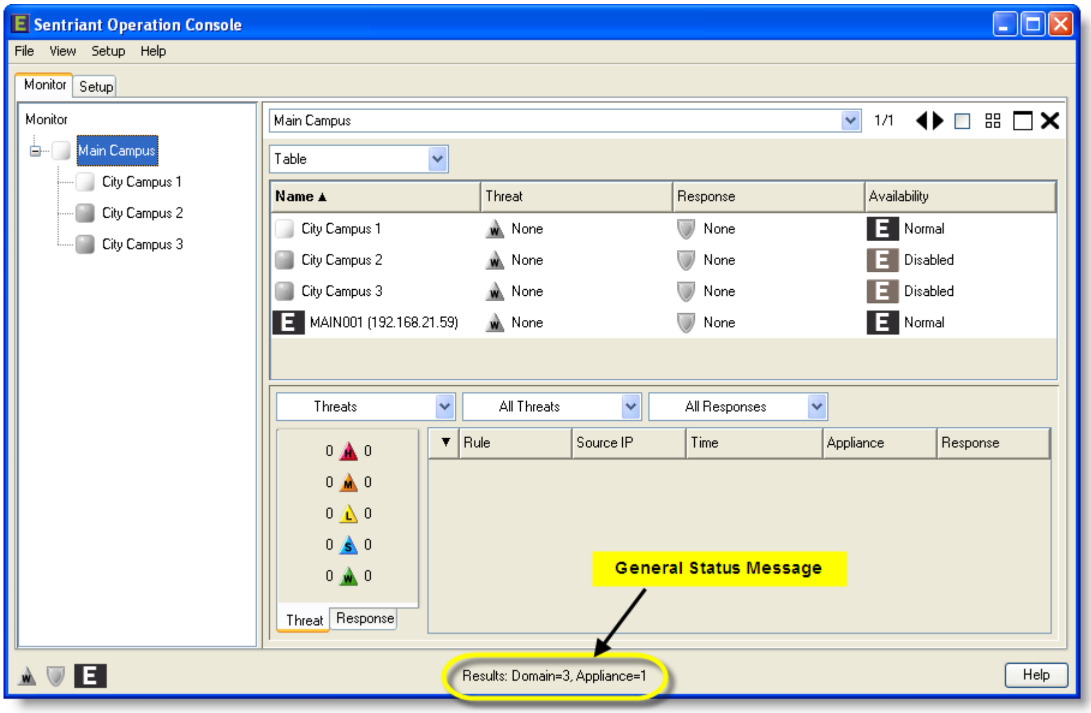
Getting Help

Sentriant Operation Console provides on-screen assistance as you move about and perform tasks by displaying messages, tips, and by clicking on the Help button to display context sensitive help. Additional information under the Help menu includes an icon legend and software version installed.

Messages and Tool Tips

Sentriant Operation Console provides brief descriptive messages that indicate what a command will do before you select the command. One kind of message is the **General Status Message** , which appears in the General Status Bar at the bottom of the screen. When you perform a command, the General Status

Message is constructed based on the command. For example, selecting a domain will display the number of domains and appliances residing within the selected domain.

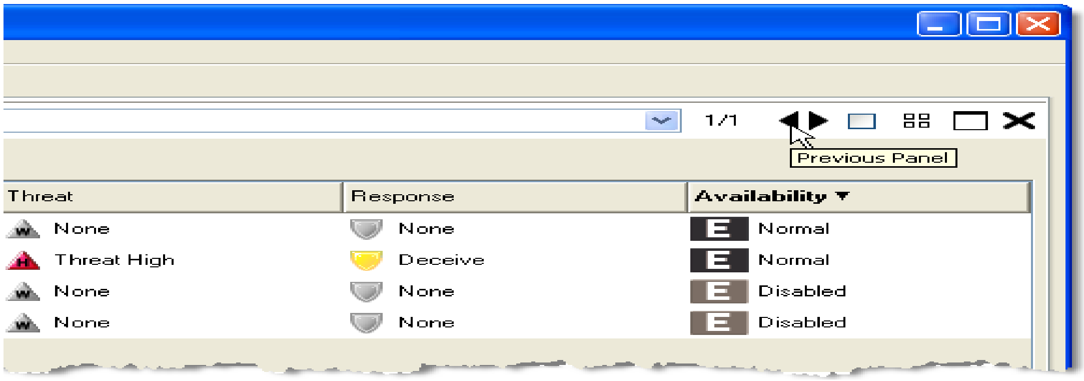


Name ▲	Threat	Response	Availability
City Campus 1	None	None	Normal
City Campus 2	None	None	Disabled
City Campus 3	None	None	Disabled
MAIN001 (192.168.21.59)	None	None	Normal

▼	Rule	Source IP	Time	Appliance	Response

Results: Domain=3, Appliance=1

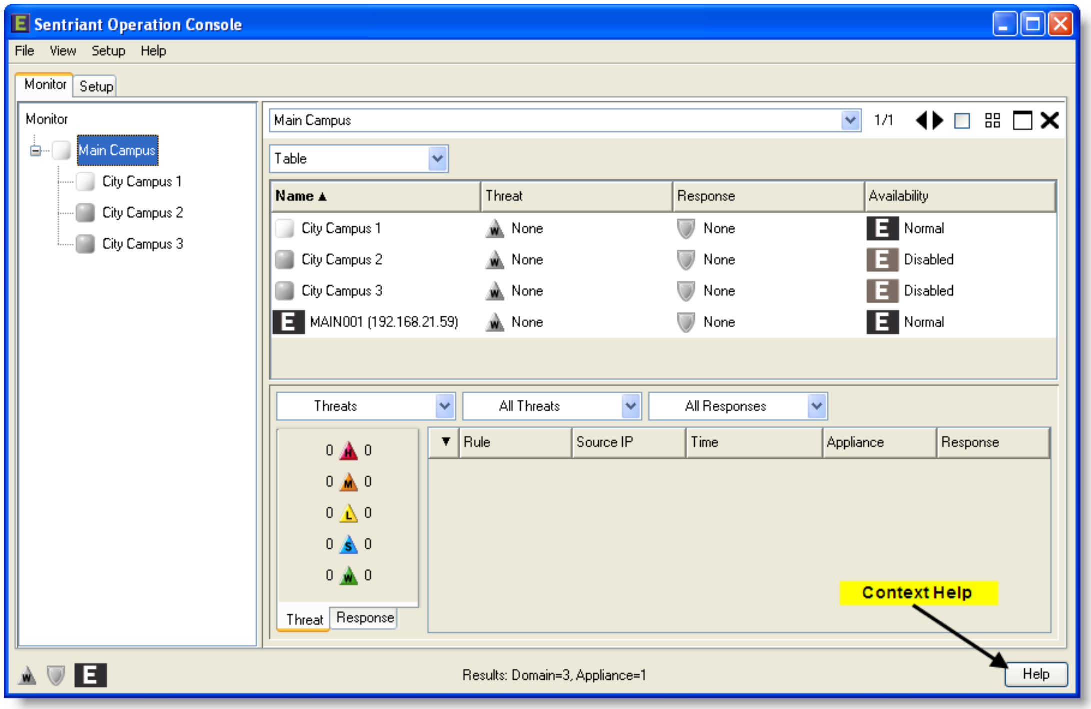
Another type of message is a **Tool Tip** , a text label describing the function of a toolbar button. Tool Tips appears when you place the pointer over a button, table field or other type of command or control.



Threat	Response	Availability ▼
None	None	Normal
Threat High	Deceive	Normal
None	None	Disabled
None	None	Disabled

Context-Sensitive Help

Context-sensitive help is also available for most of Sentriant Operation Console's information panels. The corresponding Help topic displays when you press the **Help** button located at the bottom right of the General Status Bar.



Name ▲	Threat	Response	Availability
City Campus 1	None	None	Normal
City Campus 2	None	None	Disabled
City Campus 3	None	None	Disabled
MAIN001 (192.168.21.59)	None	None	Normal

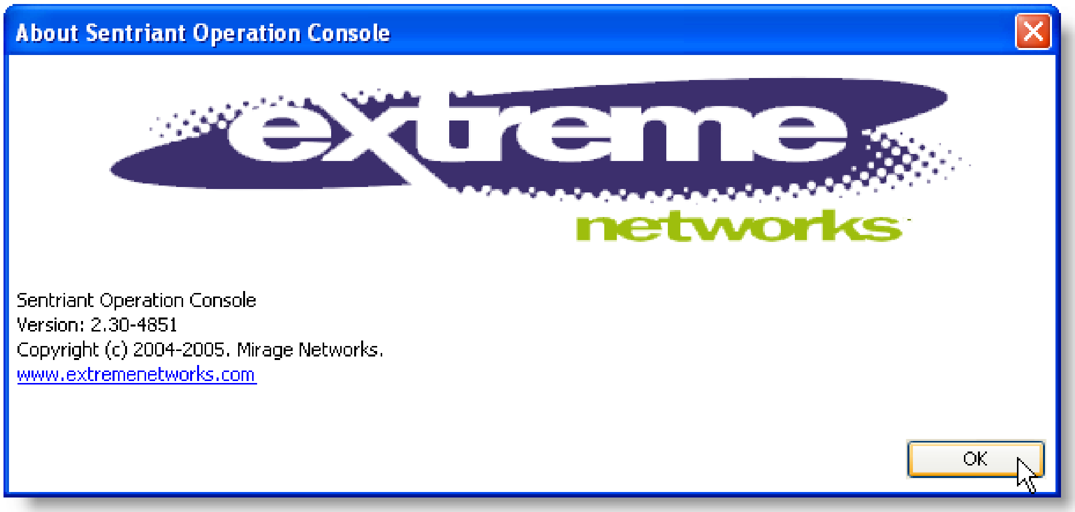
0 H	0
0 M	0
0 L	0
0 S	0
0 W	0

▼	Rule	Source IP	Time	Appliance	Response

Results: Domain=3, Appliance=1

About Sentriant Operation Console

The About command on the Help menu displays the **About Sentriant Operation Console** dialog which shows the version of Sentriant Operation Console that you are using in the title bar of the dialog.



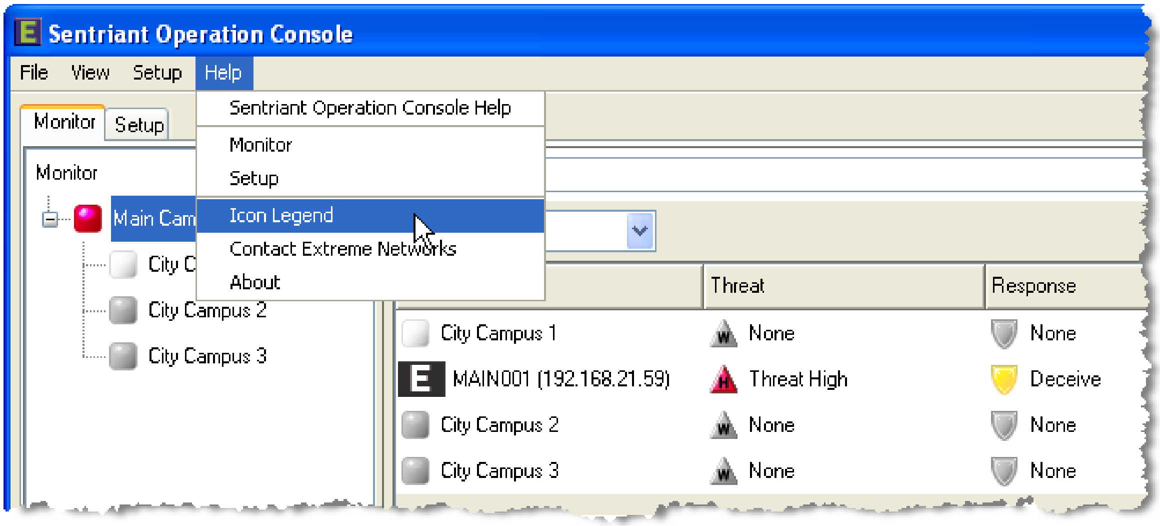
Sentriant Operation Console
Version: 2.30-4851
Copyright (c) 2004-2005. Mirage Networks.
www.extremenetworks.com

Icon Legend

An Icon Legend is provided that groups icons relative to their usage (i.e. threat priority, domain, appliance). A short description follows each icon. You may collapse or expand each group as needed.

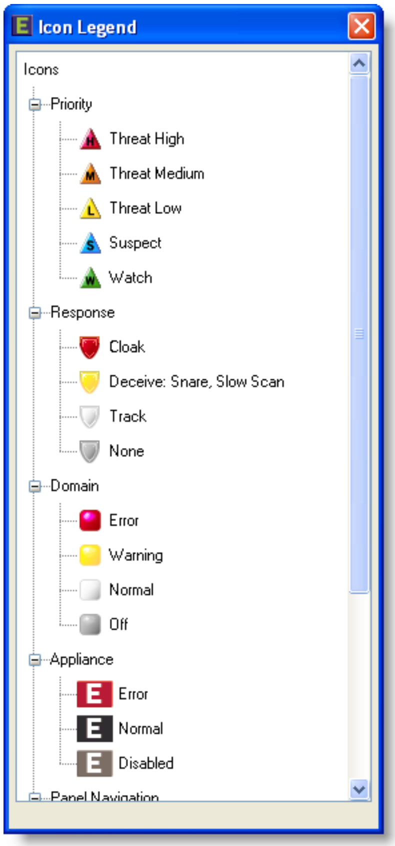
To view the Icon Legend:

1 From the Menu Bar, select Help then Icon Legend.



	Threat	Response
City Campus 1	None	None
MAIN001 (192.168.21.59)	Threat High	Deceive
City Campus 2	None	None
City Campus 3	None	None

2 Scroll down the list to see the icon categories.



Contacting Extreme Networks

Please contact Extreme Networks Support by logging into our **Technical Support Portal** at https://esupport.extremenetworks.com. The portal allows you to search the Extreme Networks knowledge base, submit a support incident, and track incidents that your organization has submitted. If you wish to speak with a support representative, call toll free at (800)-998-2408. Before calling, please create a support incident through the portal and reference the incident number.

If you report an incident with Sentriant Operation Console, please include the following information:

- Your name, E-mail, phone and fax number
- A description of the incident and what you were trying to do
- Sentriant Manager Software version number

2 Monitor

The SOC Monitor Panel provides a navigation view for ascertaining threat and appliance status across multiple domains containing multiple appliances. When SOC is launched, the Monitor Panel displays a navigation tree on the left of the screen that represents nodes of the enterprise or domains. Domains may contain sub-domains based on network deployment. Domains is where appliances are added as members of SOC that have been deployed throughout an enterprise.

Selecting a domain will display the appliances within the domain in the information panel to the right of the navigation tree. Appliance information is relayed to the operator to include the appliance name, threats detected, responses sent to threat sources, and appliance availability.

Appliance information can be viewed in two modes, a table mode that displays appliances under a single domain in a tabular view, and a radial view that displays the entire enterprise deployment graphically like the spokes of a wheel. The center of the wheel is the highest level, or root of the deployment with each spoke representing a branch of the network. Appliances are located at the end of each branch.

Threat and Response information is displayed in the details panel located at the bottom of the screen. The Threat and Response counters represent a roll up of the threats detected for the appliance. For example, if an appliance is configured to monitor four(4) segments, the Threat counter will display the total number of threats detected by the appliance. Selecting the appliance will display the type of threats and priority status. The Response counter acts similarly by rolling up the responses sent to a source threat. Filters can be set on the threat or response views to display only certain threat priorities or response types.

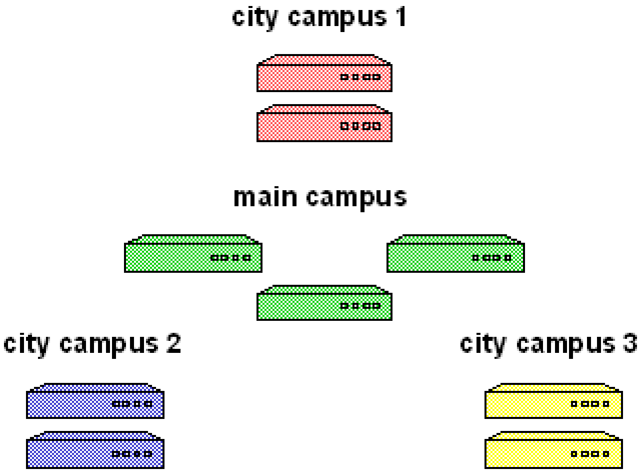
The details panel also contains a trend view. The trend view is an historical representation of threats detected by Sentriant appliances. The trend chart shows total threats and responses for an appliance. You may multi-select appliances within a domain and display an aggregate count of threats and responses.

Table View

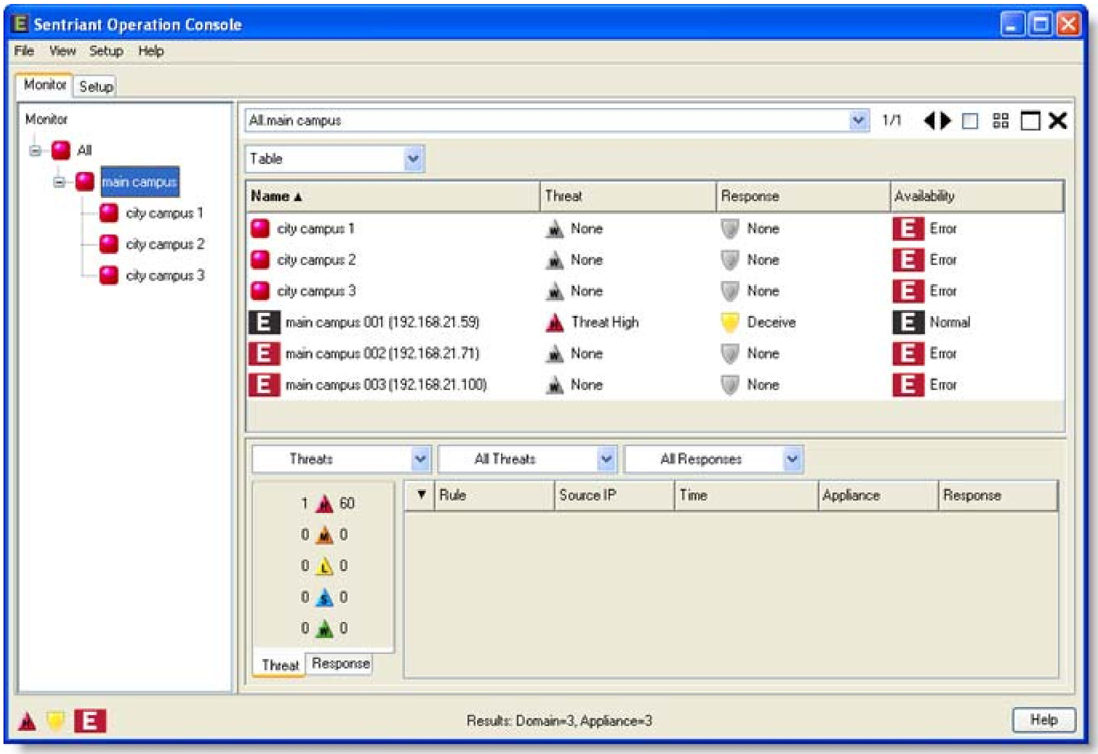
The Table View displays domains and appliance in a hierarchal list. Choosing a domain gives you sub-domains and appliances that are part of the domain. Information for domains include the name of the domain or appliance, the highest priority threat and response type for an appliance under the domain or if an appliance is selected, the highest threat detected by the appliance, and availability of the appliances within the domain or if an appliance is selected. The purpose of this panel is to provide a means of ascertaining threat and appliance status across multiple domains containing multiple appliances.

View Domains and Appliances from the Table View

The Table View displays domains which may have sub-domains. Each domain may have a single or multiple appliances assigned to it. For example, the following diagram shows an enterprise deployment to a university with a main campus, and three remote city campuses. The main campus has three Sentriant appliances deployed and each remote campus has a two Sentriant appliances deployed.



The table view will look like this:



All.main campus 1/1

Table

Name ▲	Threat	Response	Availability
city campus 1	None	None	E Error
city campus 2	None	None	E Error
city campus 3	None	None	E Error
E main campus 001 (192.168.21.59)	Threat High	Deceive	E Normal
E main campus 002 (192.168.21.71)	None	None	E Error
E main campus 003 (192.168.21.100)	None	None	E Error

Threats | All Threats | All Responses

```
1 ▲ 60
0 ▲ 0
0 ▲ 0
0 ▲ 0
0 ▲ 0
```

▼	Rule	Source IP	Time	Appliance	Response

Results: Domain=3, Appliance=3

The Table view is made up of three components - on the left of the screen is the Domains List, on the right of the screen is the Information Panel, and at the bottom of the screen is the Details Panel.

Domains List

Domains display an icon that represents the health and status of the domain. The tree displays top level domains. Clicking on the plus icon will open the folder which displays sub-domains. Domain health and status icons are as follows:

🟥 Error - A general error has been detected on an appliance that may be a high threat or the health of an appliance encountered an error. High priority threats will result in an error condition.

🟨 Warning - A warning has been detected on an appliance that may be an appliance threshold for disk space usage or a network connection went down. Suspect, low and medium priority threats will result in a warning condition.

⬜ Normal - The appliance or appliances within a domain are functioning normally. Watches may be present.

◼ Off - An appliance has stopped communicating to SOC.

Information Panel

The Information panel to the right displays sub-domains and appliances. The information panel displays the following data:

Domains/Appliances - The name of the domain or appliance with an icon representing the health and status. Appliance status icons are as follows:

E error	An error has been found with a Sentriant appliance
E warning	A warning with a Sentriant appliance
E normal	The Sentriant appliance is operating normally
E off	The Sentriant appliance is off line

Threats - A roll up of threats that have been detected. At the domain level, the roll up represents the total threats with the icon representing the highest threat priority received. Therefore, if an appliance detects 3 high and 5 medium priority threats, the counter will display the total number of the highest threat detected, in this case the icon would indicate a high threat with a count of 3. Threat priority icons are as follows:

H High - the most severe priority level. High priorities take precedence over all other priorities within SOC panels. For example, if a source has triggered a medium and high priority, only the high threat will be shown. A high can be dismissed to a watch.

M Medium - threat rules configured with medium priority take precedence over low, suspect and watches. A medium can be escalated to a high threat or dismissed to a watch.

L Low - threat rules configured with low priority take precedence over suspect and watches. A low can be escalated to a medium or high threat priority or dismissed to a watch.

S Suspect - a source that communicated with a number of unused IP Address within a protected segment. A suspect can be escalated to a Threat. A suspect can be escalated to a low, medium or high or dismissed to a watch.

W Watch - a source that communicated within a protected segment. The source may or may not reside within the segment. A watch can be escalated to a suspect, low, medium or high.

Responses - The type of response sent to the threat source. The response displayed will be determined on the type. Types of responses are Cloak, Deceive, Snare, Slow Scan, Track and none with Cloak being the most severe response against a source threat.

🛡 Cloak - A patent-pending technique by which the Sentriant appliance unilaterally controls and terminates a communications flow between two or more computers.

🛡 Deceive, Snare, and Slow Scan - Sentriant appliances use a special ‘deceiving’ technique to engage and hold TCP-based attacks, thus preventing them from spreading. Snaring stops an attacking threat from moving to another computer. Slow Scan send the attacking threat traffic designed to significantly increase the time it takes for an external host to scan the monitored network, causing the attacker to consume time and resources.

🛡 Track - A Sentriant appliance monitors the communication between two or more computers but does not take a response action.

🛡 None - No response is invoked.

Availability -The availability of the appliance or appliances under a domain. Appliances have the following availability states: Error, Normal and Disabled.

E error	An error has been found with a Sentriant appliance
E warning	A warning with the Sentriant appliance
E normal	The Sentriant appliance is operating normally
E off	The Sentriant appliance is off line

Details Panel

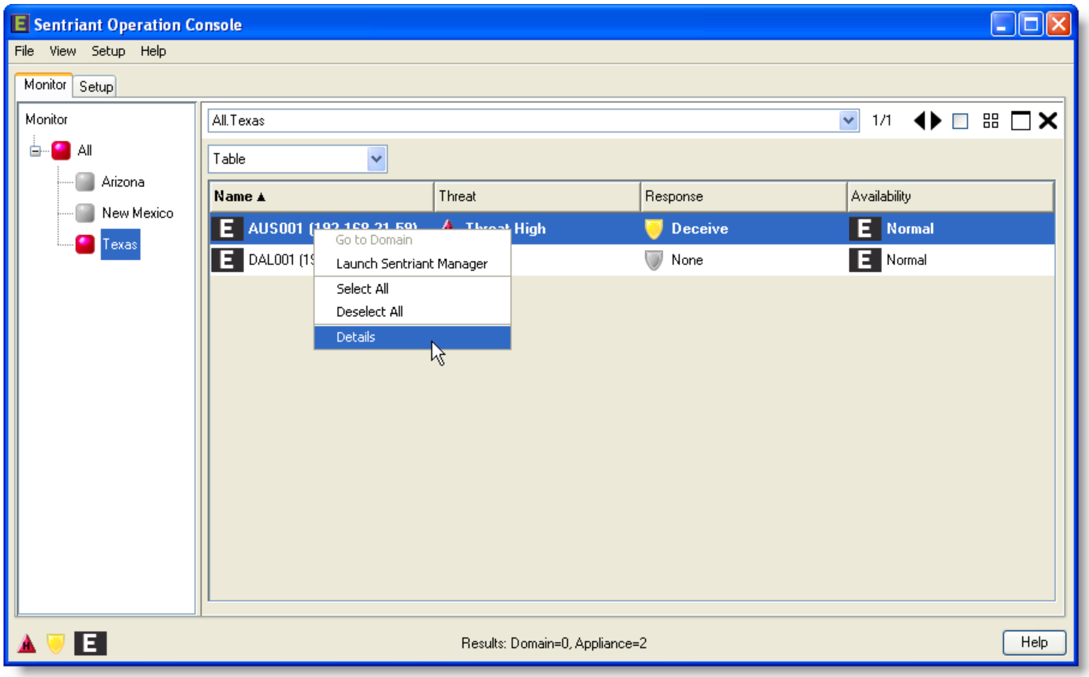
The Details Panel displays counts of threats and responses in the counter on the right of the panel. The counter can show threat and response counts for a single appliance or a roll up of threats and responses if a domain is selected. You may also multi-select domains and appliances to show a total count for the selected objects. Filters can be set to select only the threat priority and responses to be displayed in the counter. The list to the right of the counter displays threat information. Selecting Trends from the Threat/Trend drop-down list will bring up a chart. The Trend chart shows threats and responses over time and begins collecting data once the Sentriant appliances are started. Threat and response information is historical and updates periodically therefore may not match what is displayed in the counters.

Viewing Domain and Appliance Details from Table View

To view Threat Details:

1 From the Monitor Panel, select a domain from the list.

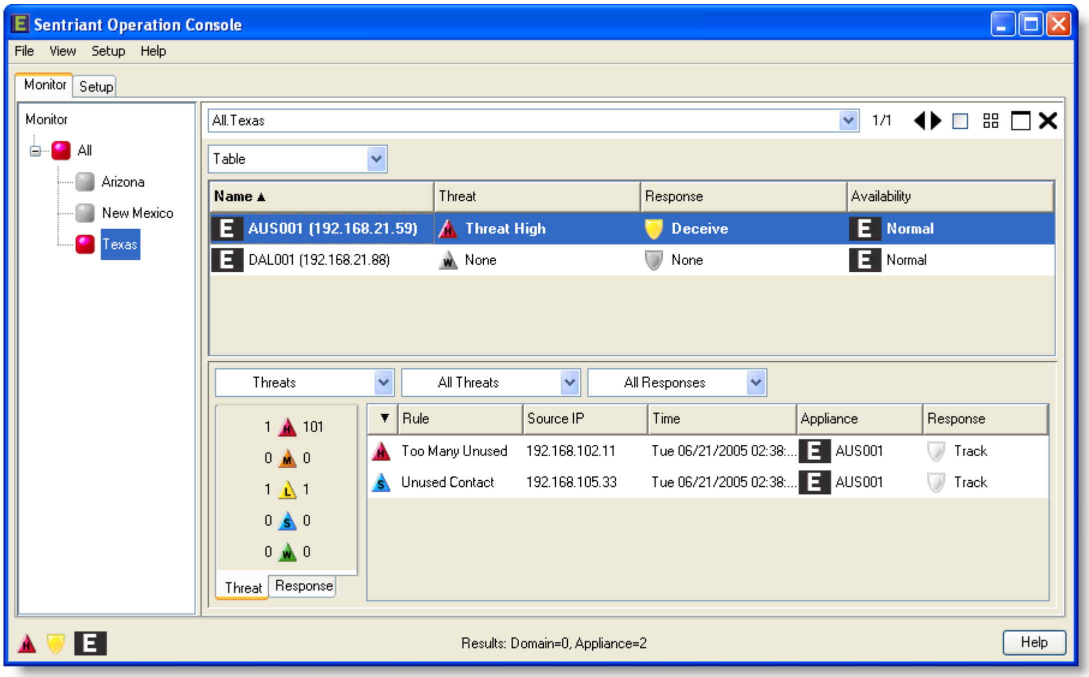
2 Double-click an appliance from the information panel or select and right-click to bring up the menu and select **Details**.



Name ▲	Threat	Response	Availability
AUS001 (192.168.21.59)	Threat High	Deceive	Normal
DAL001 (19		None	Normal

Results: Domain=0, Appliance=2

The Details Panel opens with a set of drop-down lists across the top, a threat/response counter to the right and an information list displaying active threats for the domain or appliance selected.



Name ▲	Threat	Response	Availability
AUS001 (192.168.21.59)	Threat High	Deceive	Normal
DAL001 (192.168.21.88)	None	None	Normal

1	H	101
0	M	0
1	L	1
0	S	0
0	W	0

▼	Rule	Source IP	Time	Appliance	Response
H	Too Many Unused	192.168.102.11	Tue 06/21/2005 02:38:...	AUS001	Track
S	Unused Contact	192.168.105.33	Tue 06/21/2005 02:38:...	AUS001	Track

Results: Domain=0, Appliance=2

Details Panel Drop-down Lists

Threat/Trend - The first drop-down list toggles between the Details Panel displaying the threats/ response counter and the trend chart.

Threat Filter - The second drop-down list filters the threat priorities that are displayed in the counter and information list. Selecting a threat priority will display data only for the selected priority.

Response Filter - The third drop-down list filters response types that are displayed in the counter and information list. Selecting a response type will display data only for the selected response.

Counter

The counter can be toggled between threats and responses by clicking the tabs located below the counter. The counter can show threat and response counts for a single appliance or a roll up of threats and responses if a domain is selected. You may also multi-select domains and appliances to show a total count for the selected objects.

Information List

The information list displays a breakdown of all threats detected from a domain or appliance. This view differs from the Information Panel in that the information panel show a roll up of the highest threat priority only. The detail information list displays a breakdown of all threats detected. The following data is displayed in the information list:

- threat priority
- rule that has been triggered
- source IP Address
- date and time the threat triggered
- appliance name and status
- response type taken against the threat

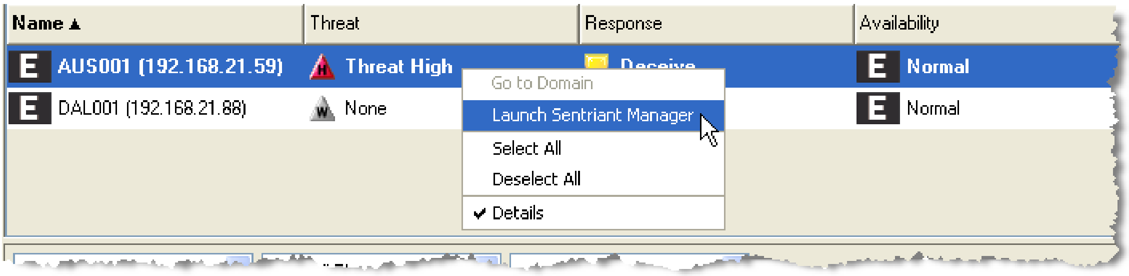
Launch Sentriant Manager from Table View

There are two locations from where you can launch Sentriant Manager.

To Launch Sentriant Manager from the Information Panel:

1 From the Monitor Panel, select an appliance from the Information Panel.

2 Right-click to bring up the menu and select **Launch Sentriant Manager**.



Name ▲	Threat	Response	Availability
E AUS001 (192.168.21.59)	Threat High	Deceive	E Normal
E DAL001 (192.168.21.88)	None		E Normal

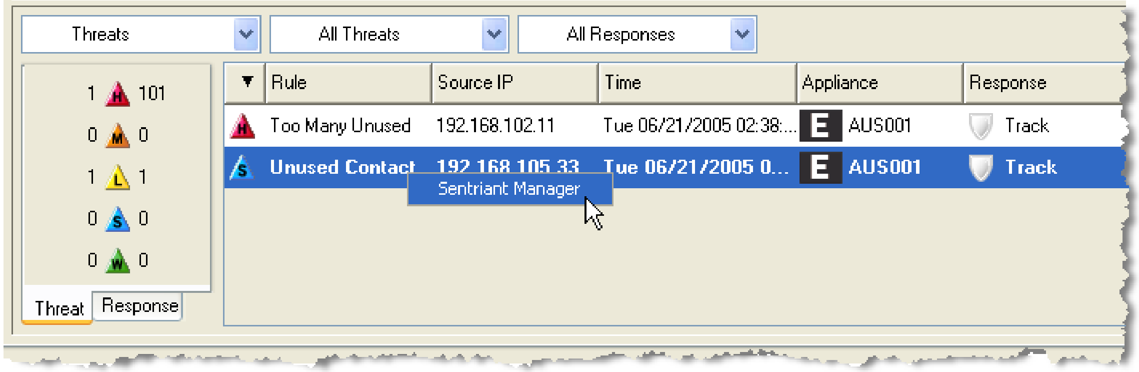
To Launch Sentriant Manager from the Details Panel:

1 From the Monitor Panel, select an appliance from the Information Panel.

2 Right-click to bring up the menu and select **Details**.

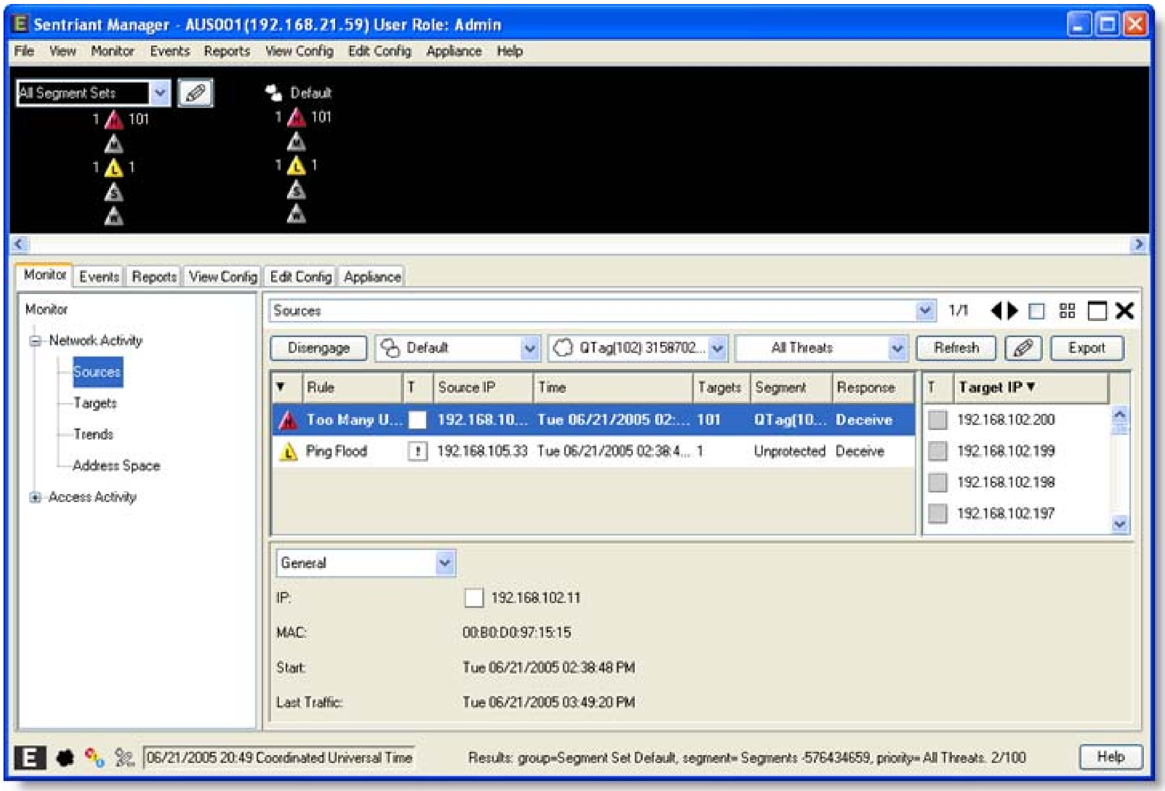
3 Select a threat from the information list.

4 Right-click to bring up the menu and select **Sentriant Manager**.



▼	Rule	Source IP	Time	Appliance	Response
H	Too Many Unused	192.168.102.11	Tue 06/21/2005 02:38:...	E AUS001	Track
S	Unused Contact	192.168.105.33	Tue 06/21/2005 0...	E AUS001	Track

The Sentriant Manager opens to Sources in the Monitor Panel.



▼	Rule	T	Source IP	Time	Targets	Segment	Response
H	Too Many U...	□	192.168.10...	Tue 06/21/2005 02:...	101	QTag(10...	Deceive
L	Ping Flood	!	192.168.105.33	Tue 06/21/2005 02:38:4...	1	Unprotected	Deceive

T	Target IP ▼
□	192.168.102.200
□	192.168.102.199
□	192.168.102.198
□	192.168.102.197

IP: □ 192.168.102.11

MAC: 00:B0:D0:97:15:15

Start: Tue 06/21/2005 02:38:48 PM

Last Traffic: Tue 06/21/2005 03:49:20 PM

06/21/2005 20:49 Coordinated Universal Time

Results: group=Segment Set Default, segment= Segments -576434659, priority= All Threats. 2/100

Radial View

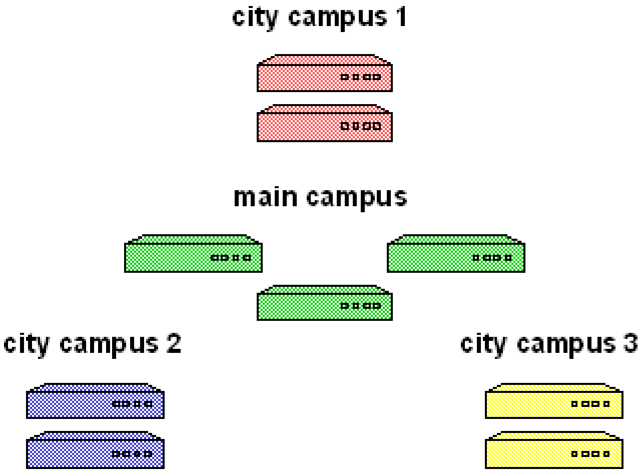
The radial view displays the entire enterprise deployment graphically like the spokes of a wheel. The center of the wheel is the highest level, or root of the deployment with each spoke representing a branch of the network. Appliances are located at the end of each branch.

The Radial View displays domains and appliance in a graphical view. Clicking a domain displays the sub-domains and appliances that are part of the domain. Clicking a sub-domain displays the appliances of the sub-domain. Clicking an appliance will display icons for threats, responses and availability of the appliance. The purpose of this panel is to provide a means of ascertaining threats, responses, and appliance status within a large deployment that reside in many domains.

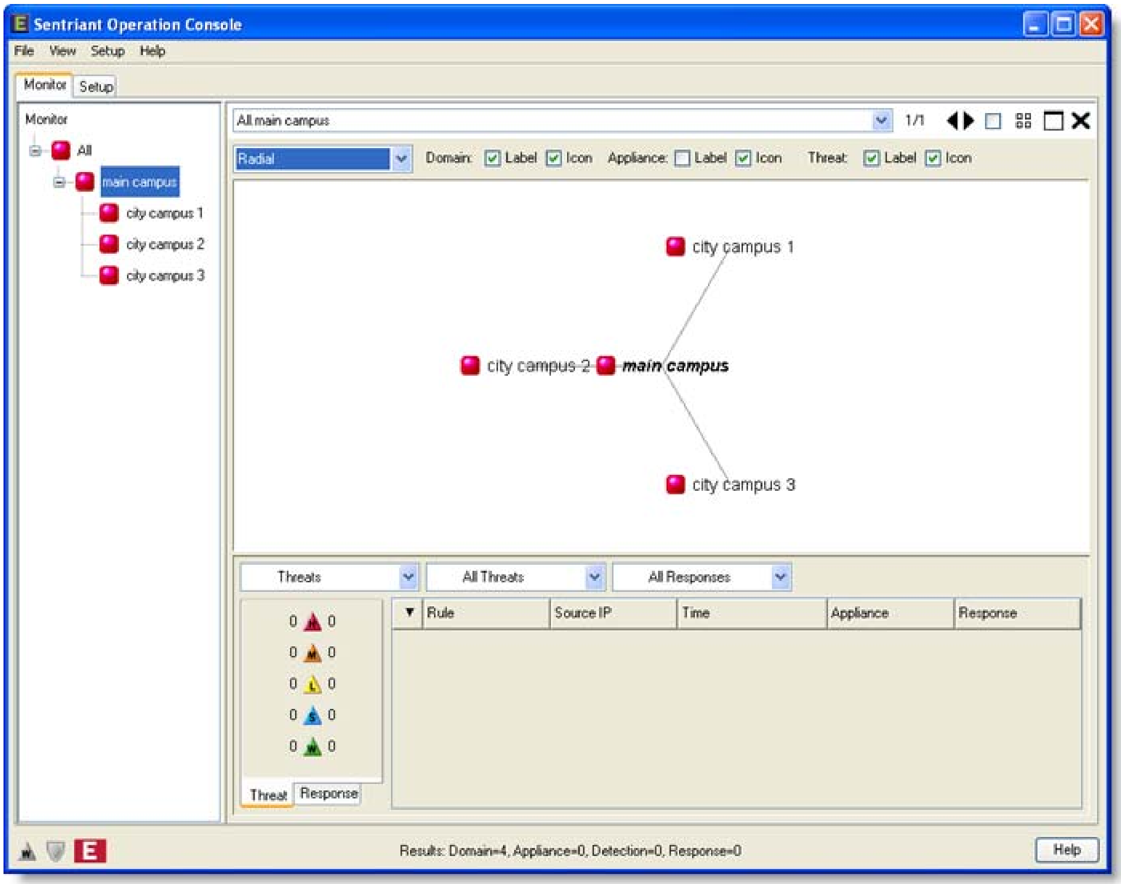
The main difference from the table and radial views is that you can display sub-domains and appliances in one view and determine which domain or appliance has detected threats. Once the appliance has been determined, you can move to it quickly without having to navigate through a tree.

View Domains and Appliances from the Radial View

The radial view displays the entire enterprise deployment graphically like the spokes of a wheel. The center of the wheel is the highest level, or root of the deployment with each spoke representing a branch of the network. Appliances are located at the end of each branch. The benefits of the Radial view is where there is a large deployment of appliances that reside in many domains. For example, the following diagram shows an enterprise deployment to a university with a main campus, and three remote city campuses. The main campus has three Sentriant appliances deployed and each remote campus has a two Sentriant appliances deployed.



The radial view will look like this:



Results: Domain=4, Appliance=0, Detection=0, Response=0

The Radial view gives the operator a high level view of all Sentriant appliances deployed and then can drill down or filter to the appliance detecting threats by double clicking on a domain and then the appliance. Domains display an icon that represents the health and status of the domain. Domain health and status icons are as follows:

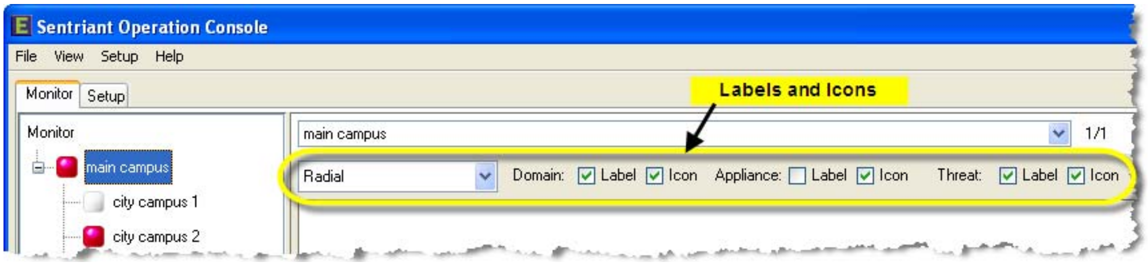
🔴 Error - A general error has been detected on an appliance that may be a high threat has been detected on an appliance or the health of an appliance encountered an error. High priority threats will result in an error condition.

🟡 Warning - A warning has been detected on an appliance that may be an appliance threshold for disk space usage or a network connection went down. Suspect, low and medium priority threats will result in a warning condition.

⚪ Normal - The appliance or appliances within a domain are functioning normally. Watches may be present.

● Off - An appliance has stopped communicating with SOC.

Across the top of the information panel is a set of check boxes that turn on and off radial view labels and icons. Turning on and off labels and icons will make reading the radial view easier if you have an environment with many domains and appliances.



The Information panel displays domains and appliances. The information panel displays the following data:

- The name of the domain or appliance with an icon representing the health and status
- A roll up of threats that have been detected. At the domain level, the roll up represents the total threats with the icon representing the highest threat priority received. Therefore, if an appliance detects 3 high and 5 medium priority threats, the counter will display the total number of the highest threat detected, in this case the icon would indicate a high threat with a count of 3.
- The type of response sent to the threat source. The response displayed will be determined by the type. Types of responses are Cloak, Deceive, Snare, Slow Scan, Track and none with Cloak being the most severe response against a source threat.
- The availability of the appliance or appliances under a domain. Appliances have the following availability states, Error, Normal and Disabled.

View Domain and Appliance Details from the Radial View

Threat and response details can be view in a number of ways from the Radial view depending on what is selected at different levels. For example, selecting the highest level in the radial view, in the case below 'main campus', all threats and responses will be displayed in the Details Panel for all appliances. Selecting a sub-domain within 'main campus' will only show threats and responses in that domain. Selecting an appliance will only show threats and responses for the appliance selected.

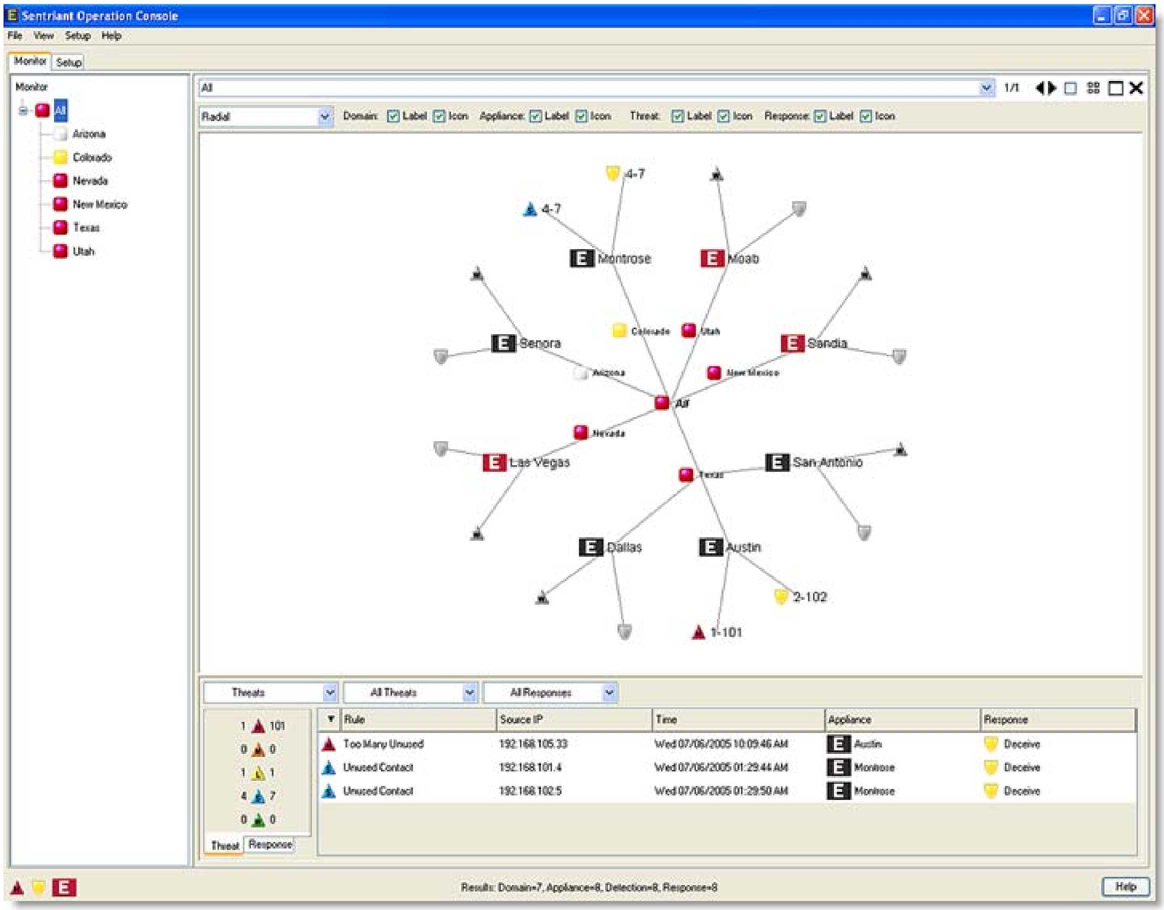
To View Threat Details:

From the Monitor Panel, select a domain from the list.

NOTE

By default, the details panel is turned on. If the Details Panel has be turned off, it can be turned on by right-clicking in the information panel and selecting Details from the menu.

The Details Panel opens with a set of drop-down lists across the top, a threat/response counter to the right and an information list displaying active threats for the domain or appliance selected.



All

Radial Domain: ☑ Label ☑ Icon Appliance: ☑ Label ☑ Icon Threat: ☑ Label ☑ Icon Response: ☑ Label ☑ Icon

Threats | All Threats | All Responses

1	101
0	0
1	1
4	7
0	0

Rule	Source IP	Time	Appliance	Response
Too Many Unused	192.168.105.33	Wed 07/06/2005 10:09:46 AM	Austin	Deceive
Unused Contact	192.168.101.4	Wed 07/06/2005 01:29:44 AM	Montrose	Deceive
Unused Contact	192.168.102.5	Wed 07/06/2005 01:29:50 AM	Montrose	Deceive

Results: Domain=7, Appliance=8, Detection=8, Response=8

Details Panel Drop-down Lists

Threat/Trend - The first drop-down list toggles the Details Panel between displaying the threats/ response counter and list to the trend chart.

Threat Filter - The second drop-down list filters the threat priorities that are displayed in the counter and information list. Selecting a threat priority will display data only for the selected priority.

Response Filter - The third drop-down list filters response types that are displayed in the counter and information list. Selecting a response type will display data only for the selected response.

Counters

Counters can be toggled between threats and responses by clicking the tabs located below the counter. The counter can show threat and response counts for a single appliance or a roll up of threats and responses if a domain is selected.

Information List

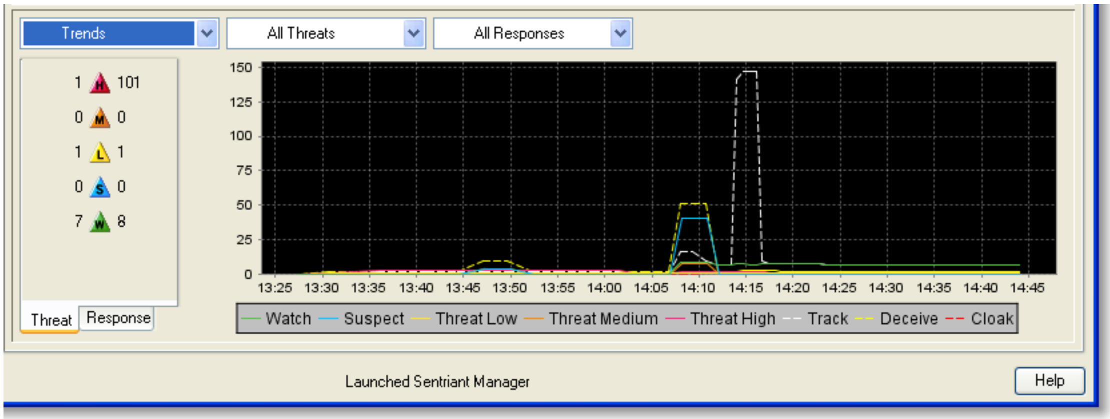
The information list displays a breakdown of all threats detected from a domain or appliance. This view differs from the Information Panel in that the information panel show a roll up of the highest threat priority only. The detail information list displays a breakdown of all threats detected. The following data is displayed in the information list:

- threat priority will show the highest threat priority for a source, however the source may have triggered lower priority threats.
- name of the rule that has been broken
- source IP Address
- date and time the threat triggered
- status and name of the appliance that received a threat
- response type taken against the threat

Right-clicking a threat in the list and selecting **Sentriant Manager** will launch Sentriant Manager and will open the Monitor > Network Activity > Sources Panel.

Trend Chart

The Trend Chart represent a historical view of threats/responses. The data displayed depends on what is selected in the Radial View.



Launched Sentriant Manager

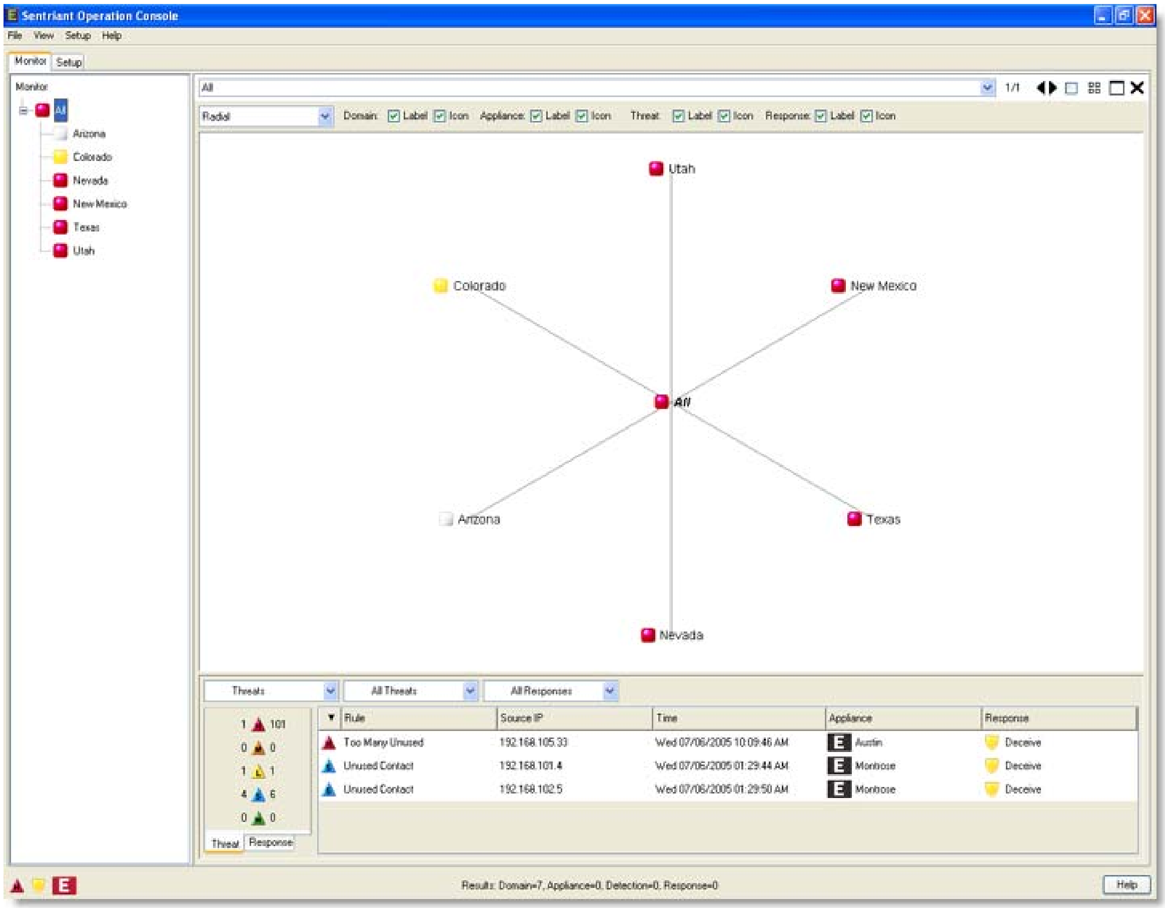
Showing Appliances

The default Radial view shows the root and first level domains and hides appliances and sub-level domains. When a threat is detected or there is a warning or error with an appliance, the domain icons will change status alerting you that there is activity. You can then filter down to where the activity occurred. The example below shows there is an error in the Texas domain and a warning in the Colorado domain.

NOTE

The root, in this case All will display an error icon. The more severe domain status will be displayed at the root.

With **All** selected, the Details Panel at the bottom of the panel shows all threats detected for all appliances.

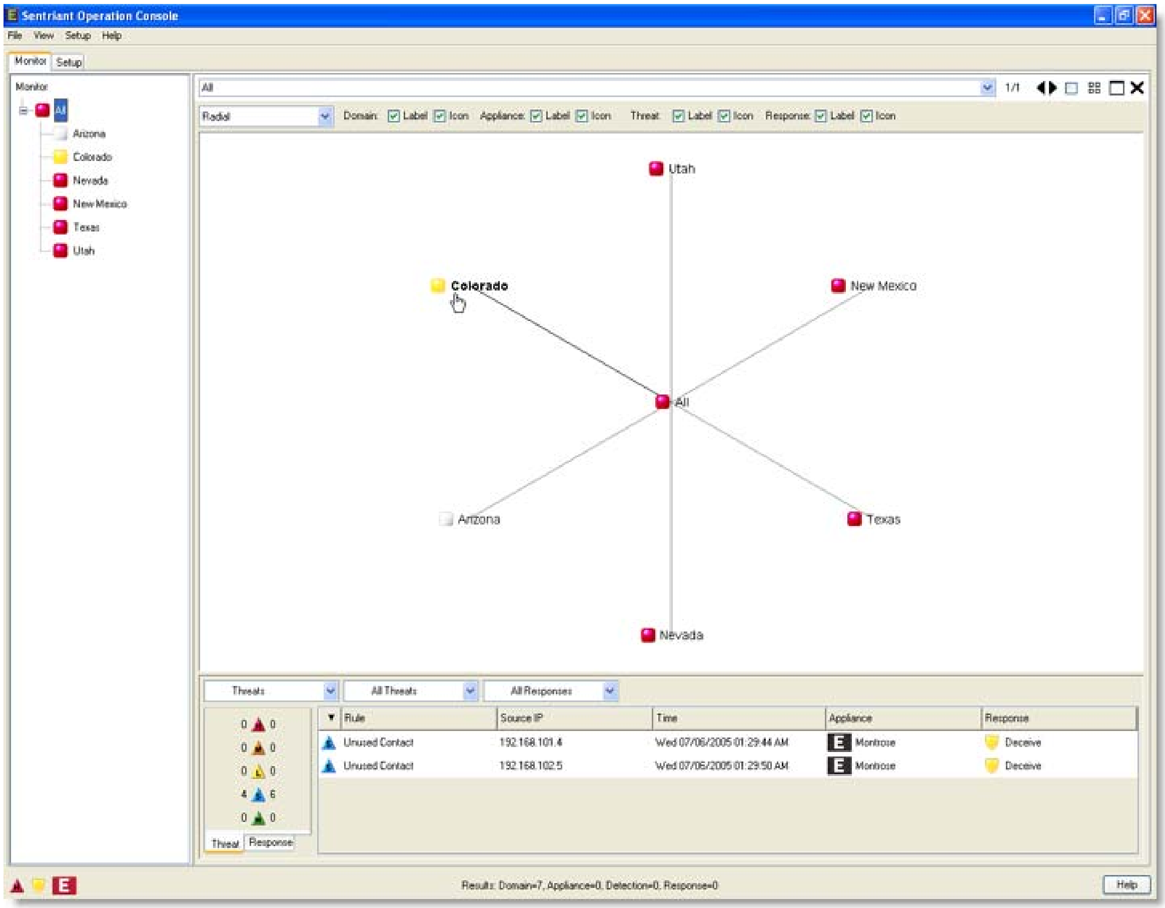


Domain: ☑ Label ☑ Icon Appliance: ☑ Label ☑ Icon Threat: ☑ Label ☑ Icon Response: ☑ Label ☑ Icon

Rule	Source IP	Time	Appliance	Response
Too Many Unused	192.168.105.33	Wed 07/06/2005 10:09:46 AM	Austin	Deceive
Unused Contact	192.168.101.4	Wed 07/06/2005 01:29:44 AM	Montrose	Deceive
Unused Contact	192.168.102.5	Wed 07/06/2005 01:29:50 AM	Montrose	Deceive

Results: Domain=7, Appliance=0, Detection=0, Response=0

Clicking a domain, in this case **Colorado**, will display threats detected from appliance only within the Colorado domain.



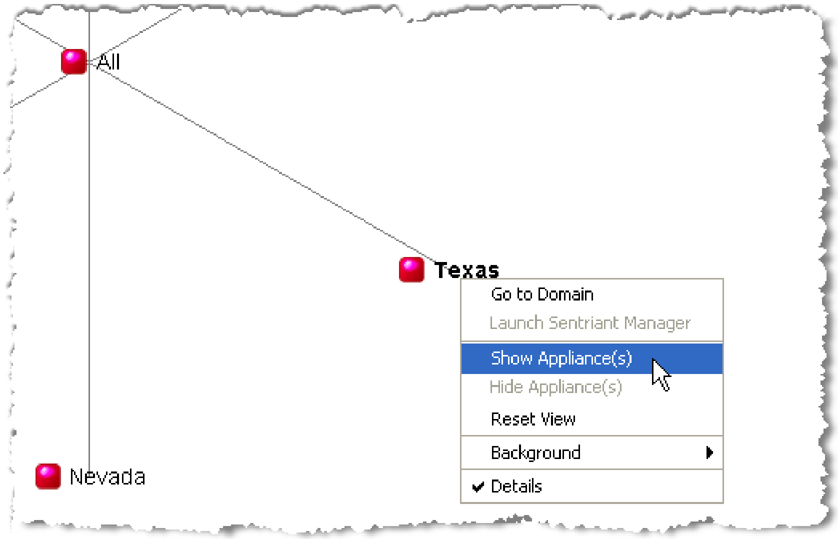
	Rule	Source IP	Time	Appliance	Response
	Unused Contact	192.168.101.4	Wed 07/06/2005 01:29:44 AM	Montrose	Deceive
	Unused Contact	192.168.102.5	Wed 07/06/2005 01:29:50 AM	Montrose	Deceive

Results: Domain=7, Appliance=0, Detection=0, Response=0

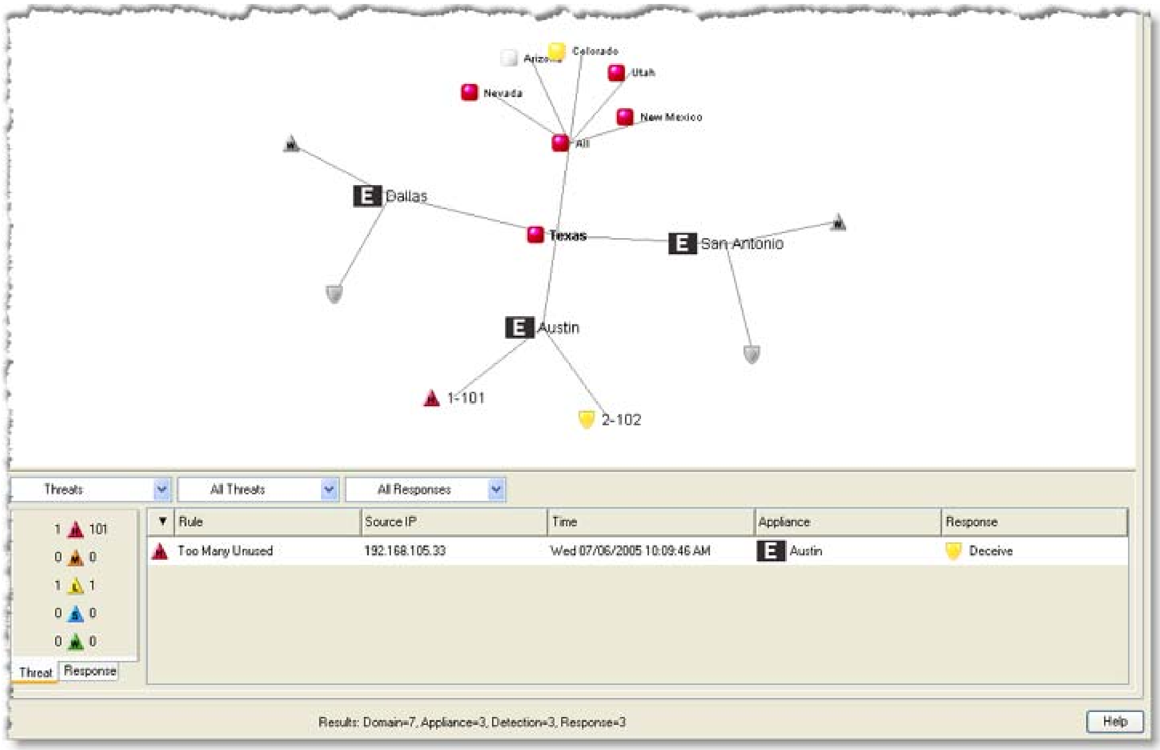
All information to this point has been at the domain level which represents a roll up of all appliances. To view individual appliance information you may show appliances within a domain.

To show appliances:

Right-click a domain and select **Show Appliance(s)**.



The appliances for the selected domain are displayed with threat and response counters. In the example below, the appliance named Austin shows that it has detected one threat that is targeting 101 workstation within the protected segments. The details panel displays the threat rule that has been triggered, the sources IP Address, a timestamp when the threat triggered the rule, the status and name of the appliance and response type sent to the source.



1 ▲	101
0 ▲	0
1 ▲	1
0 ▲	0
0 ▲	0

▼	Rule	Source IP	Time	Appliance	Response
▲	Too Many Unused	192.168.105.33	Wed 07/06/2005 10:09:46 AM	E Austin	Deceive

Results: Domain=7, Appliance=3, Detection=3, Response=3

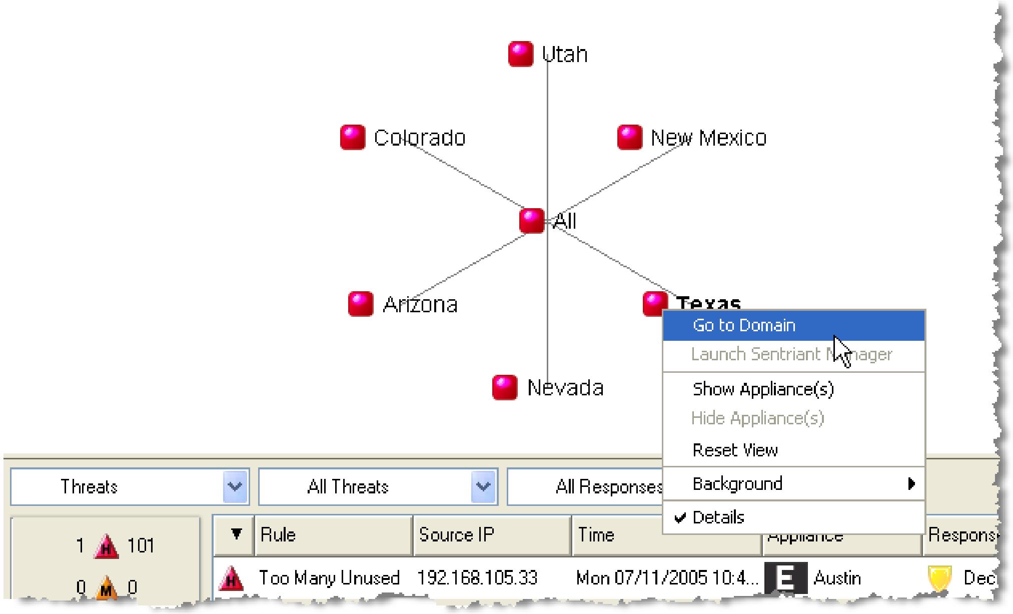
Radial View Actions

You may perform actions on the radial view, domain, and appliances by right-clicking in the radial view. Below are the available actions:

Go To Domain.

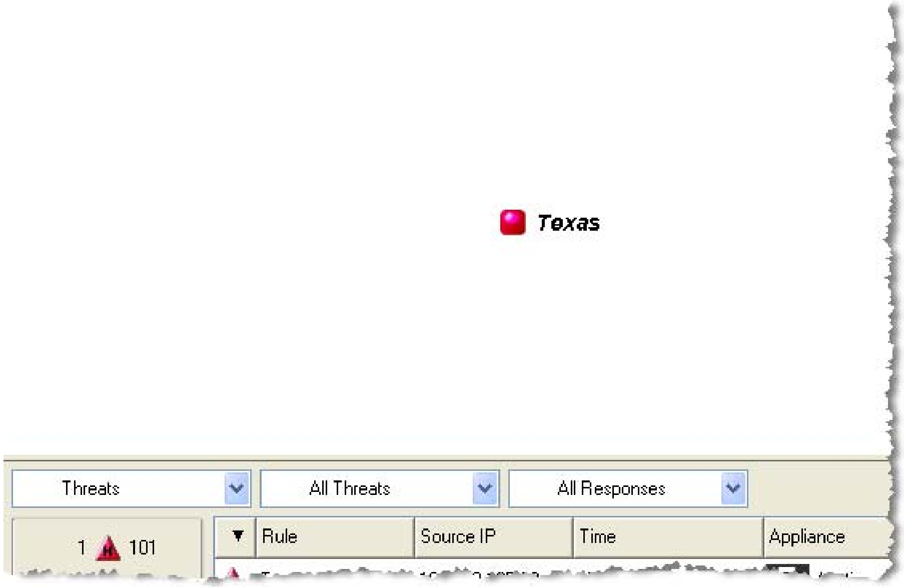
The **Go to Domain** action will navigate to the domain selected.

1 Right-click a domain from the Radial view.
2 Select **Go to Domain** from the menu.



Rule	Source IP	Time	Appliance	Respons
Too Many Unused	192.168.105.33	Mon 07/11/2005 10:4...	E Austin	Dec

The Radial view is now focused on the selected domain.

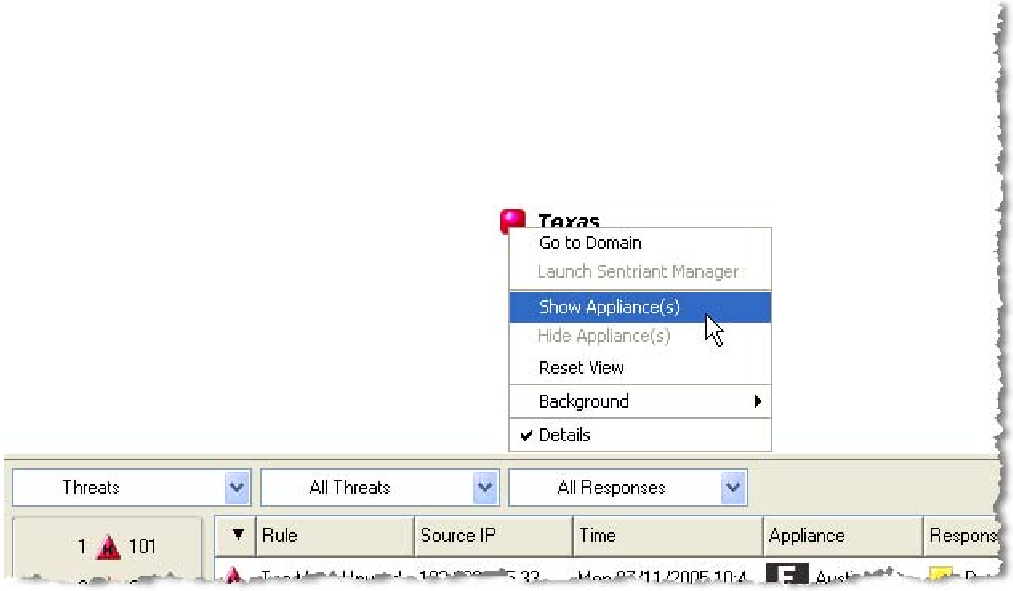


Show Appliances.

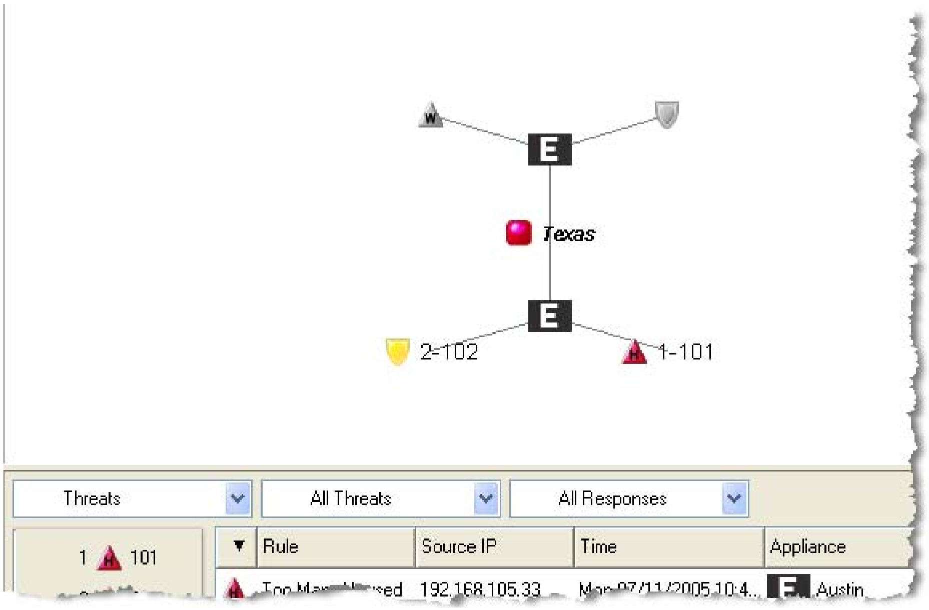
Sentriant appliances are not displayed to preserve Radial view's space. In a large deployment with many domains, it may be necessary to only show the domains. To show the appliances within a domain:

1 Right-click a domain from the Radial view.

2 Select **Show Appliance(s)** from the menu.



The appliance(s) within the domain are displayed.

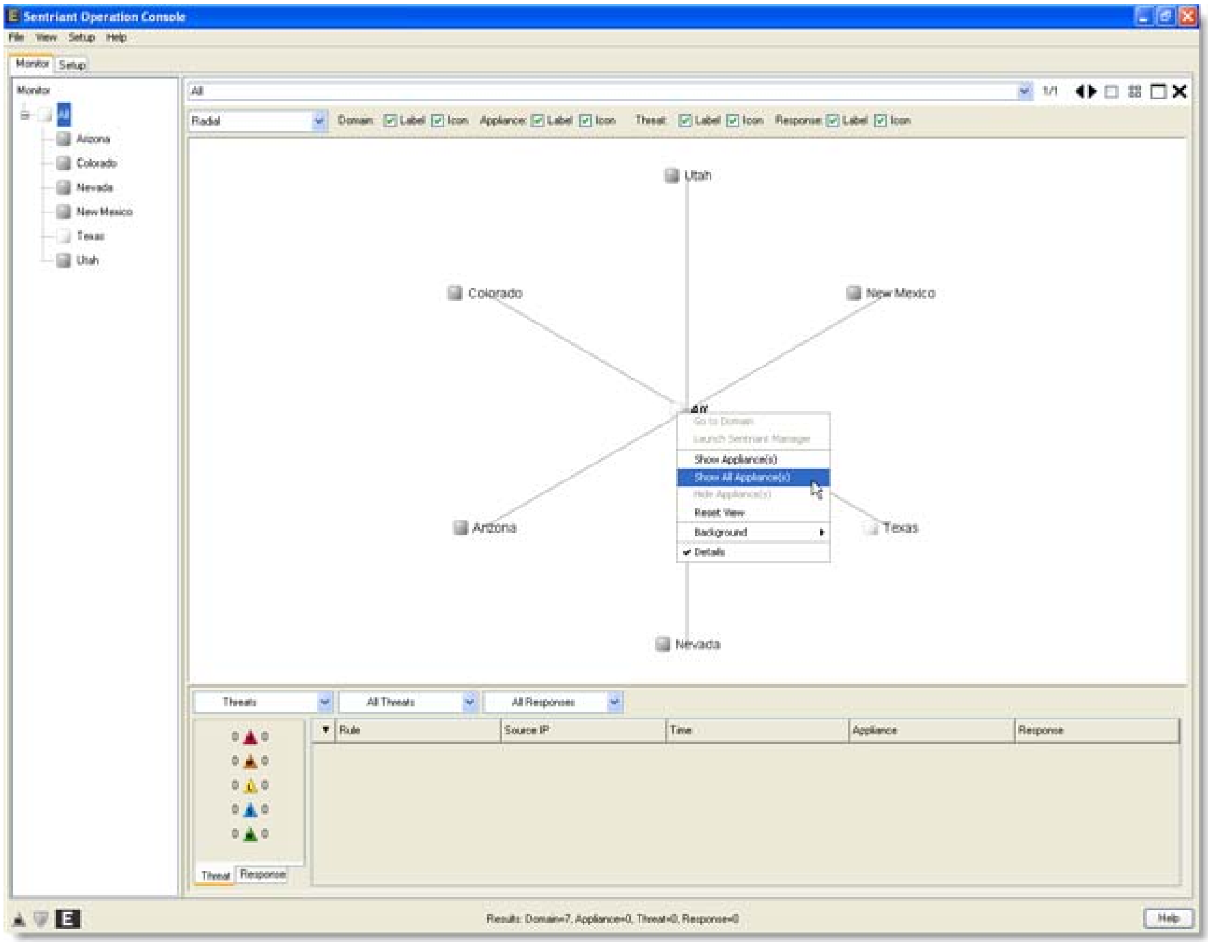


Show All Appliances.

In a small deployment, it may be beneficial to view all Sentriants in all the domains. To show all the appliances within all domains:

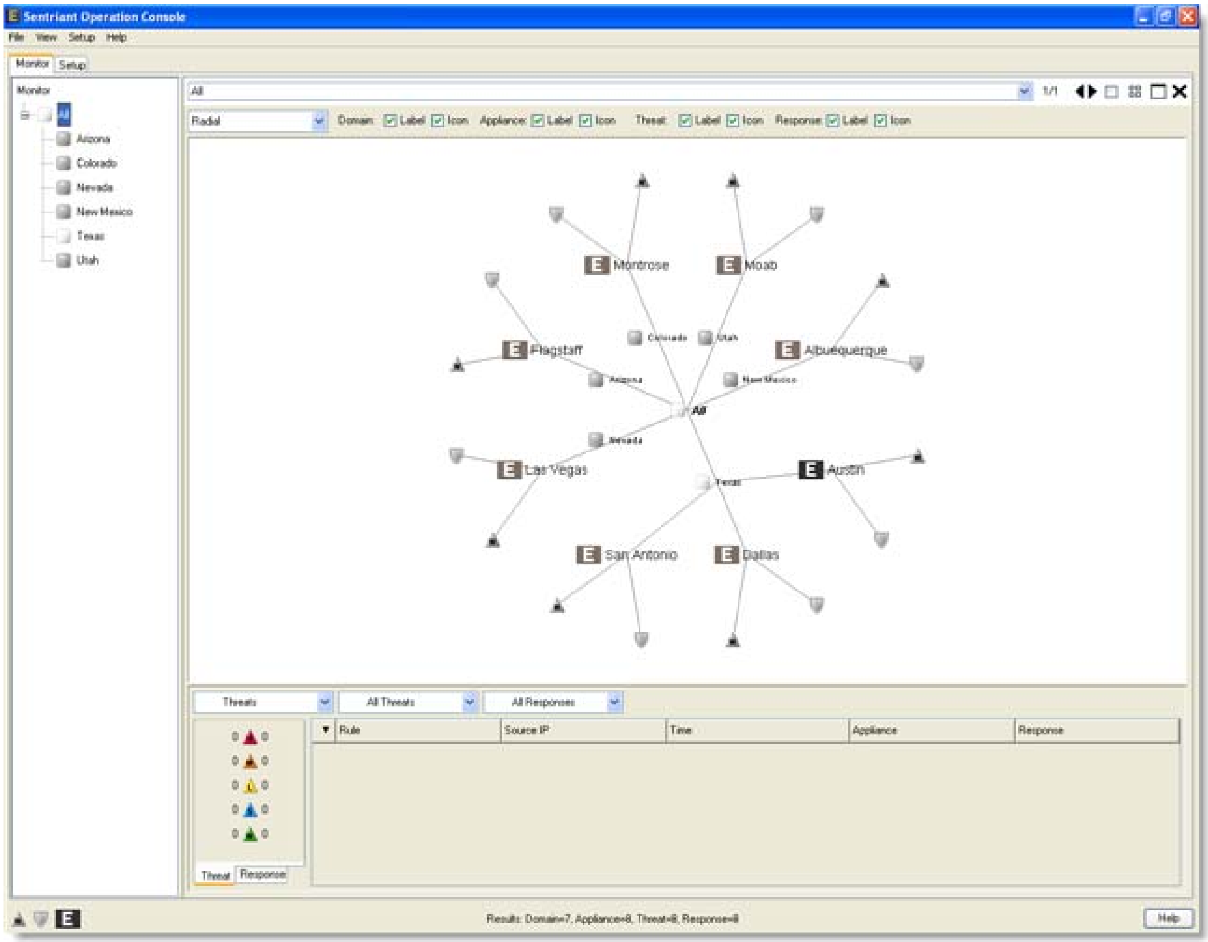
1 Right-click in the Radial view panel.

2 Select Show All Appliance(s) from the menu.



Results: Domain=7, Appliance=0, Threat=0, Response=0

All appliances in all domains are displayed.



All

Radial Domain: ☑ Label ☑ Icon Appliance: ☑ Label ☑ Icon Threat: ☑ Label ☑ Icon Response: ☑ Label ☑ Icon

Threats | All Threats | All Responses

▼	Rule	Source IP	Time	Appliance	Response

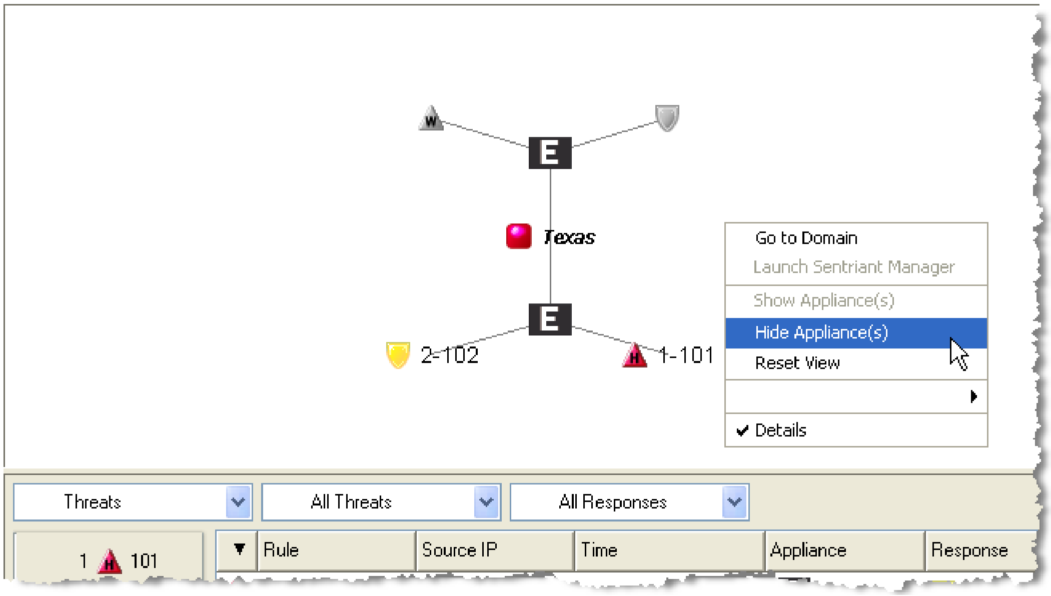
Results: Domain=7, Appliance=8, Threat=8, Response=8

Hide Appliances.

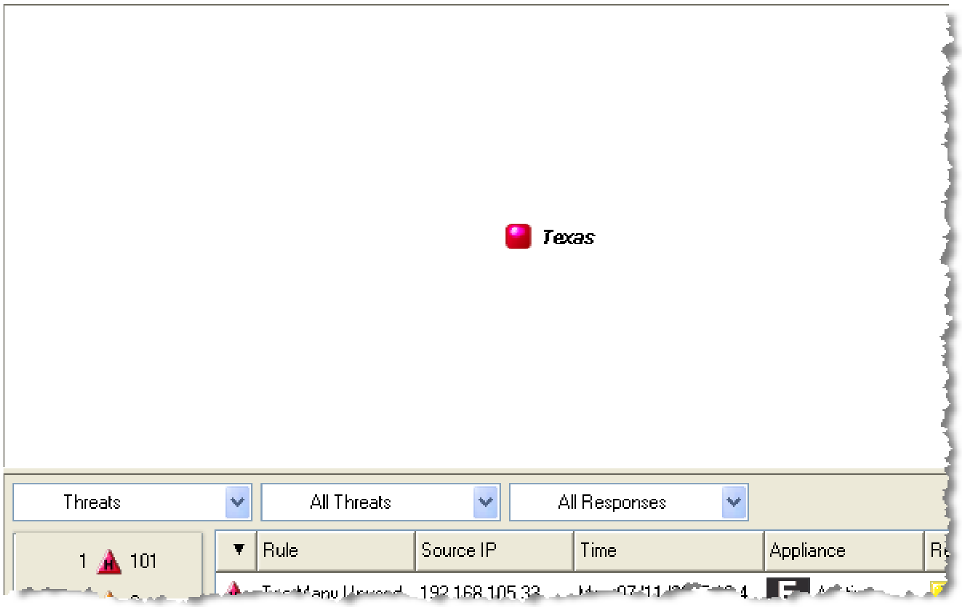
If it is no longer necessary to show appliances or you need more space to display another domain's appliances, you can hide appliances.

1 Right-click a domain from the Radial view.

2 Select **Hide Appliance(s)** from the menu.



The appliance(s) within the domain are hidden.

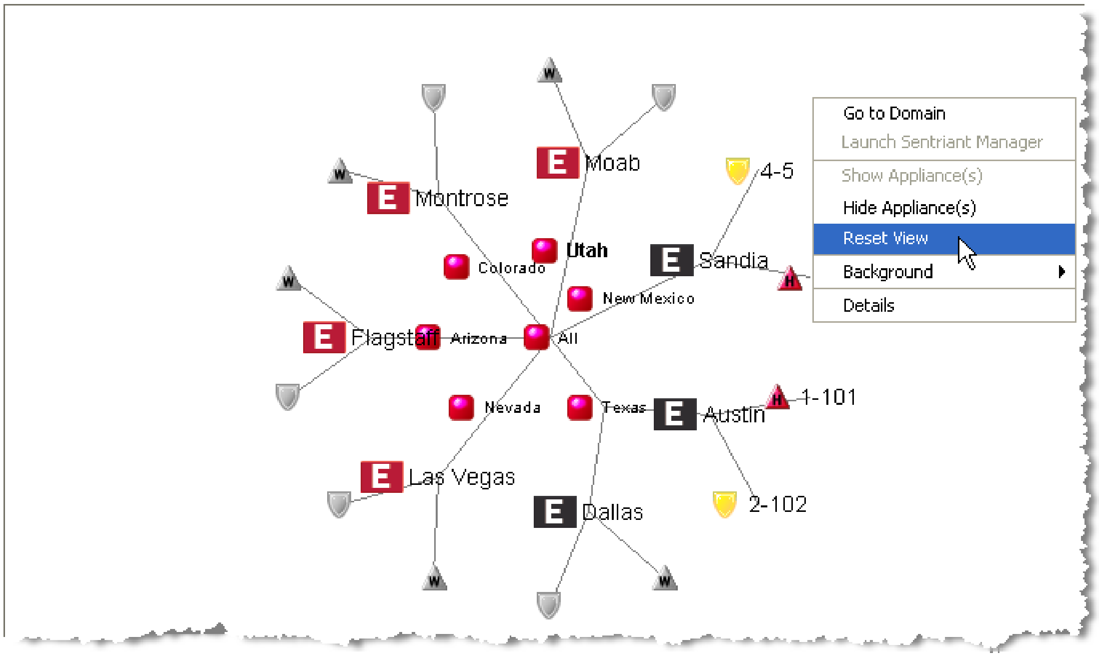


Reset View.

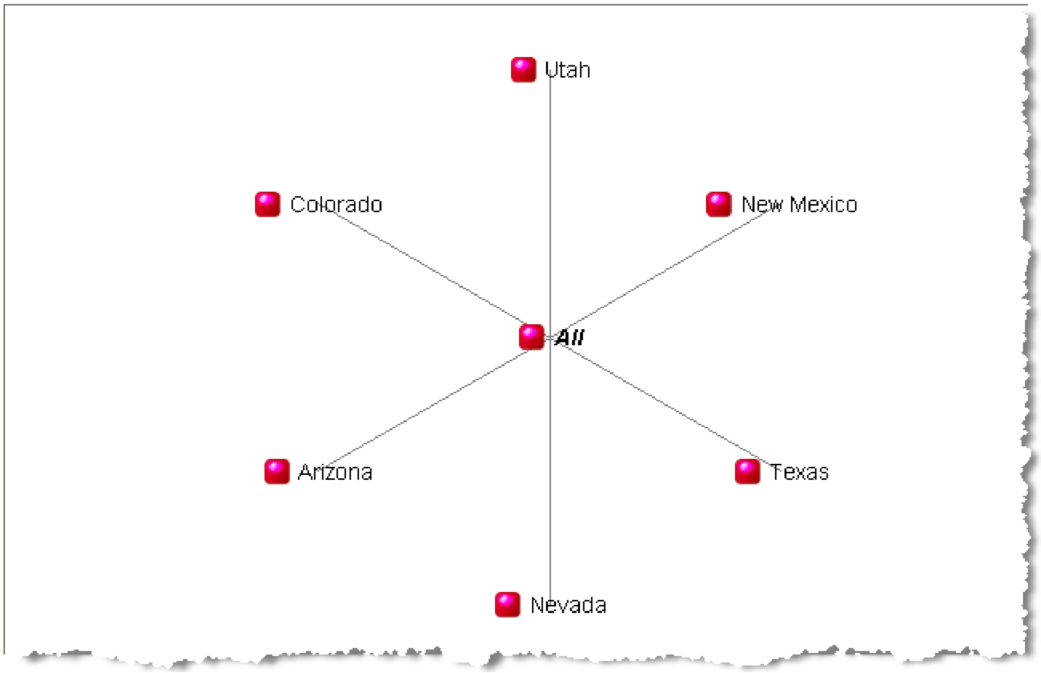
Resetting the view allows you to reset the Radial view showing the highest domain level and second level sub-domains. For example, if you are showing third level sub-domains and/or appliance, click the Reset View action will reset the view to display only the highest level domain and second level sub-domains. Third and lower domains and appliances will be hidden.

1 Right-click a domain from the Radial view.

2 Select **Reset View** from the menu.



The Radial view returns to the default view of showing highest domain level and second level sub-domains.



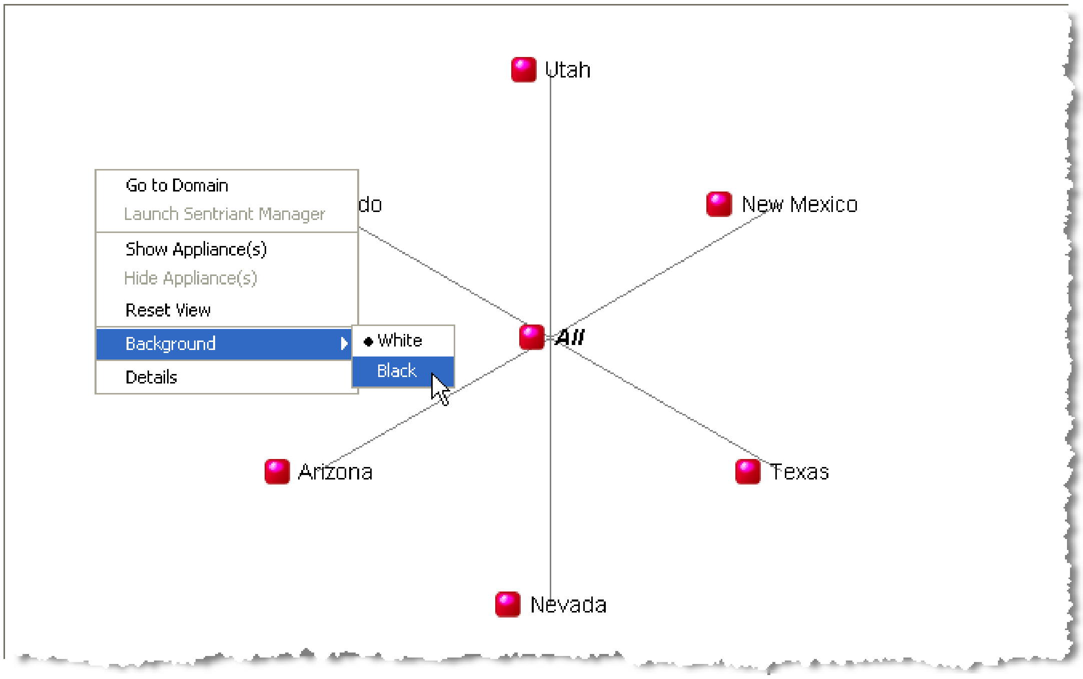
Change Background.

You may change the color of the Radial view's background from white to black.

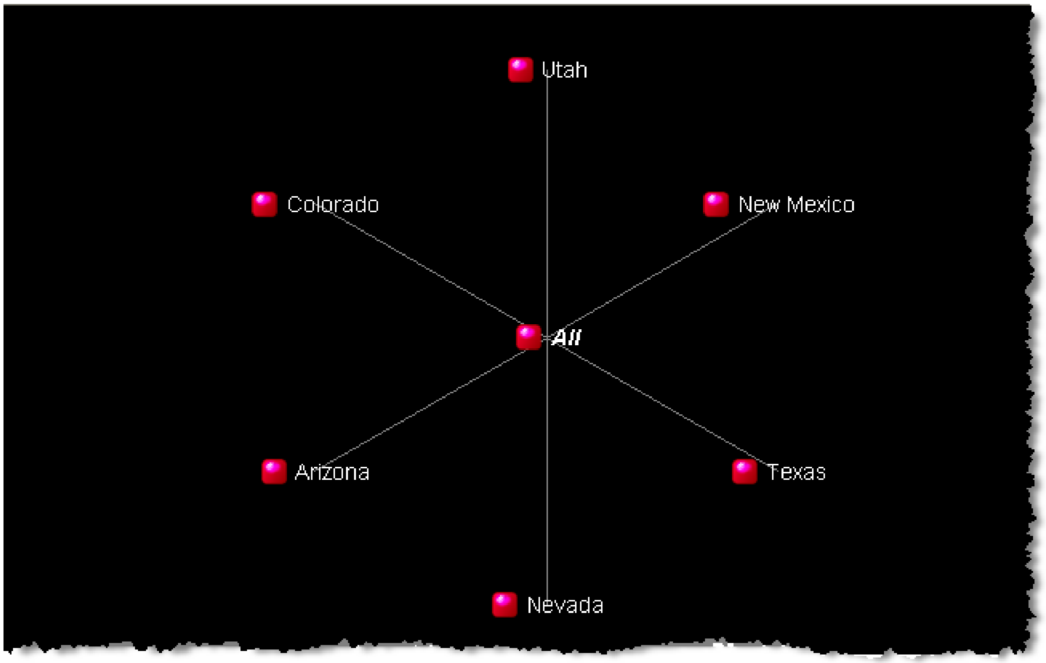
1 Right-click a domain from the Radial view.

2 Select **Background** from the menu.

3 Select either **White** or **Black**.



The Radial view's background changes.



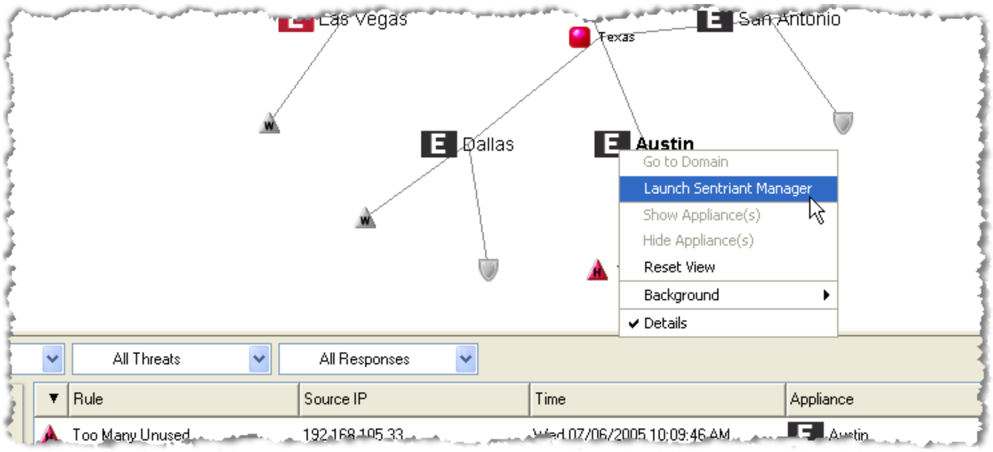
Launch Sentriant Manager from Radial View

There are two locations from where you can launch Sentriant Manager.

To Launch Sentriant Manager from the Radial View:

1 From the Monitor Panel, select an appliance from the Information Panel.

2 Right-click to bring up the menu and select **Launch Sentriant Manager**.



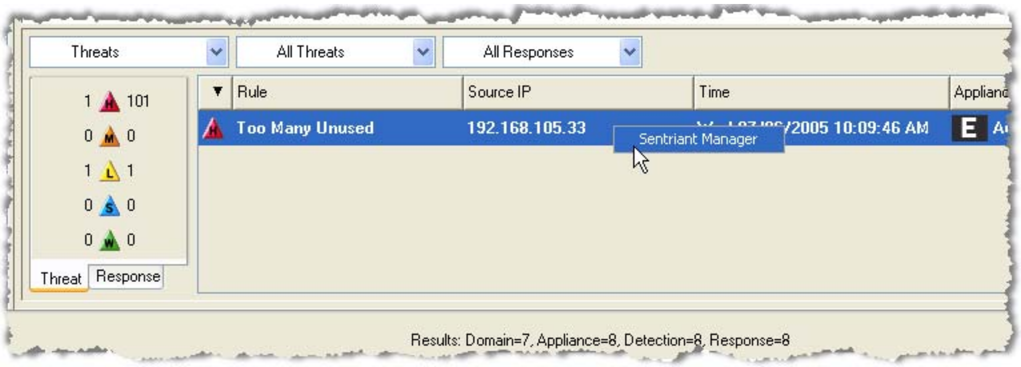
Rule	Source IP	Time	Appliance
Too Many Unused	192.168.105.33	Wed 07/06/2005 10:09:46 AM	Austin

To Launch Sentriant Manager from the Details Panel:

1 From the Monitor Panel, select an appliance from the Information Panel.

2 Select a threat from the information list.

3 Right-click to bring up the menu and select **Sentriant Manager**.

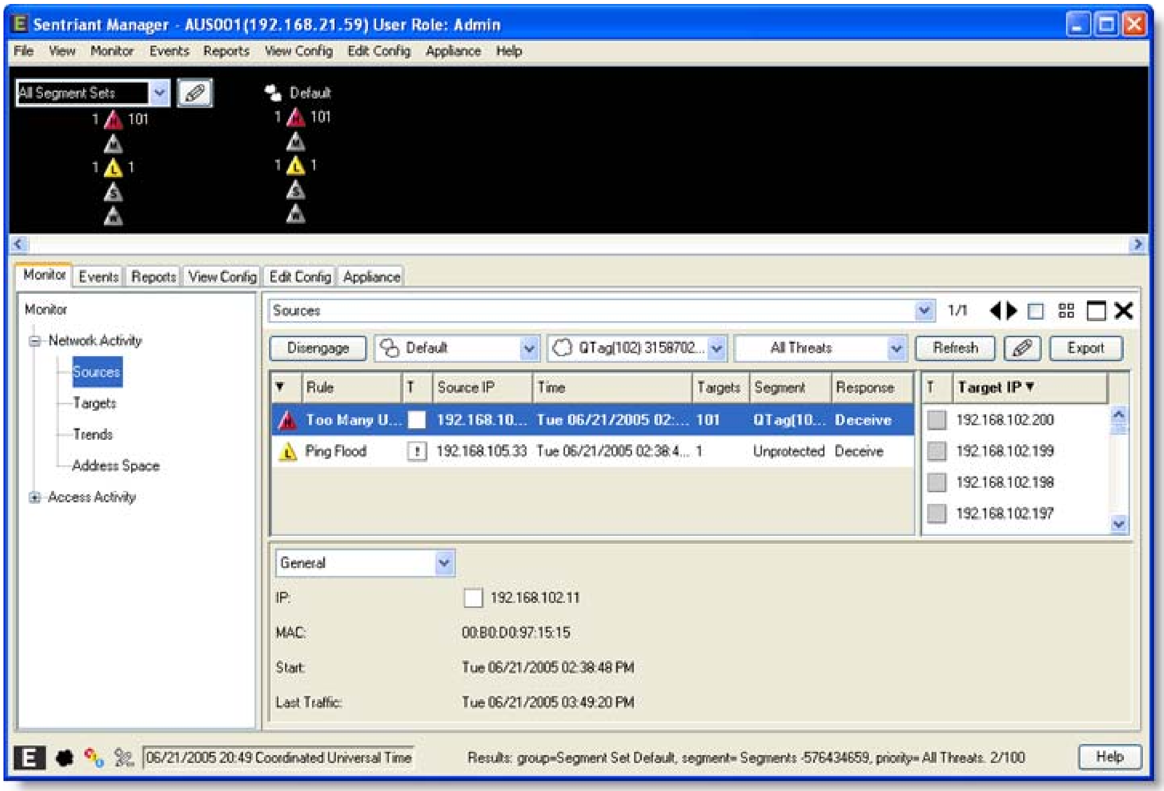


1	H	101
0	M	0
1	L	1
0	S	0
0	W	0

Rule	Source IP	Time	Applianc
Too Many Unused	192.168.105.33	/2005 10:09:46 AM	E Au

Results: Domain=7, Appliance=8, Detection=8, Response=8

The Sentriant Manager opens to Sources in the Monitor Panel.



▼	Rule	T	Source IP	Time	Targets	Segment	Response
	Too Many U...	□	192.168.10...	Tue 06/21/2005 02:...	101	QTag(10...	Deceive
	Ping Flood	!	192.168.105.33	Tue 06/21/2005 02:38:4...	1	Unprotected	Deceive

T	Target IP ▼
□	192.168.102.200
□	192.168.102.199
□	192.168.102.198
□	192.168.102.197

IP: □ 192.168.102.11

MAC: 00:80:D0:97:15:15

Start: Tue 06/21/2005 02:38:48 PM

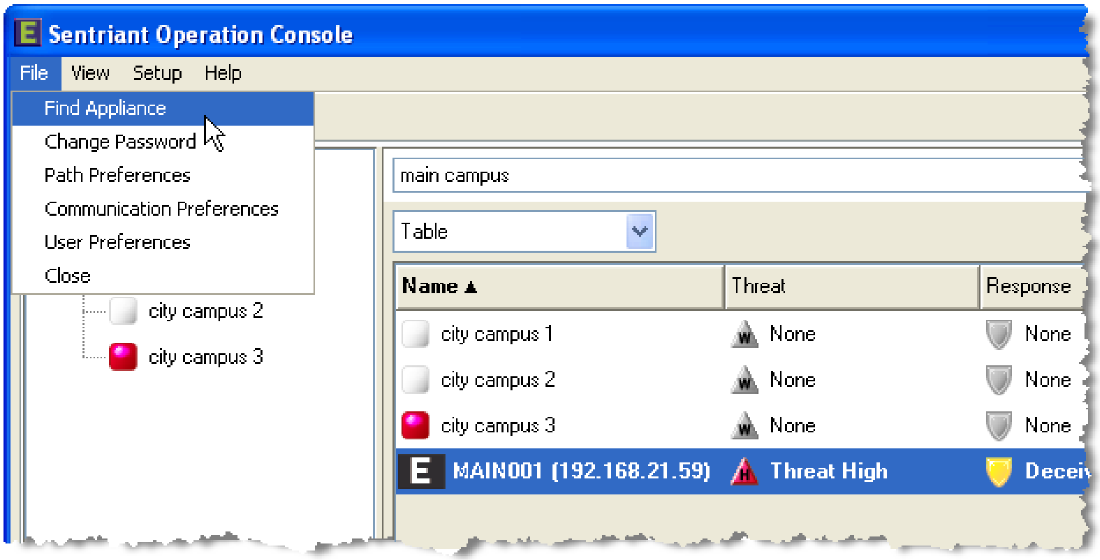
Last Traffic: Tue 06/21/2005 03:49:20 PM

Results: group=Segment Set Default, segment= Segments -576434659, priority= All Threats. 2/100

Finding Appliances

To find appliance or appliances:

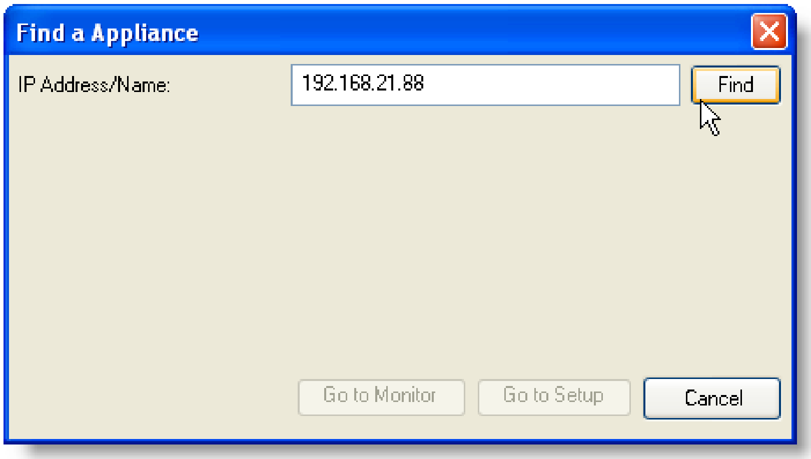
1 From the Menu, select **File > Find Appliance**.



Name ▲	Threat	Response
city campus 1	None	None
city campus 2	None	None
city campus 3	None	None
MAIN001 (192.168.21.59)	Threat High	Decei

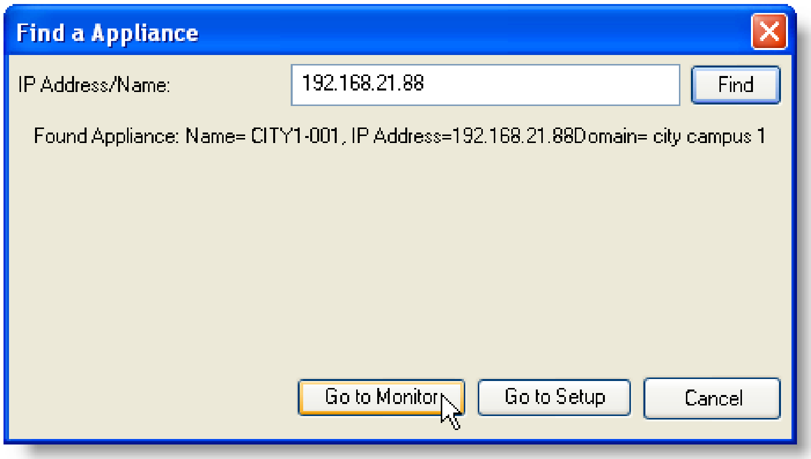
2 Enter the IP Address or name of the appliance.

3 Click **Find**.



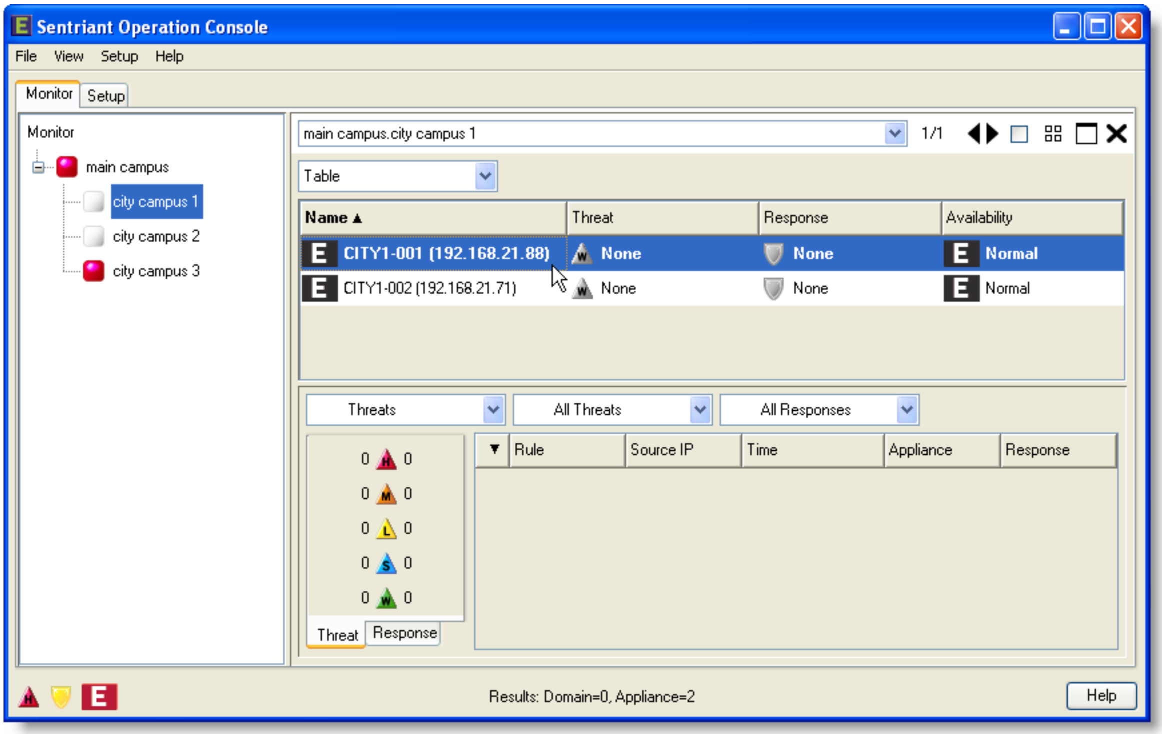
A message is displayed with the Name, IP Address and the Domain where the appliance is located.

4 Click either the **Go to Monitor** or **Go to Setup** to navigate to the appliance.



Found Appliance: Name= CITY1-001, IP Address=192.168.21.88Domain= city campus 1

Depending on which button is clicked will take you the either the Monitor or Setup panel with the appliance highlighted.



Name ▲	Threat	Response	Availability
CITY1-001 (192.168.21.88)	None	None	Normal
CITY1-002 (192.168.21.71)	None	None	Normal

▼	Rule	Source IP	Time	Appliance	Response

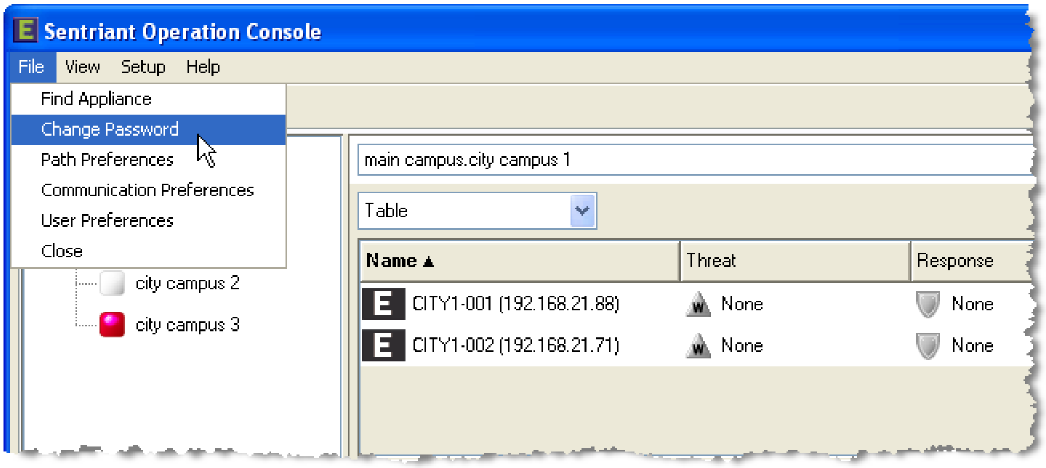
Setting Preferences

The Sentriant Operation Console is installed with pre-defined settings for password, paths, communications and user preferences. Settings may be customized as necessary.

Changing Password

To change SOC password:

1 From the Menu, select **File > Change Password**.

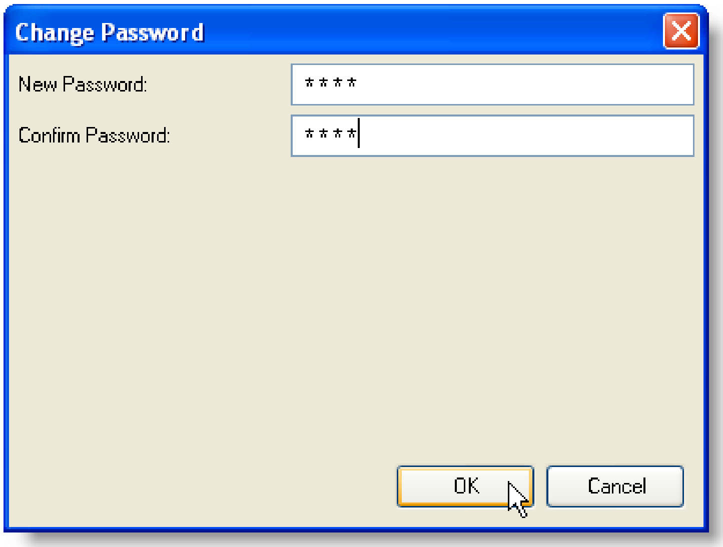


Name ▲	Threat	Response
CITY1-001 (192.168.21.88)	None	None
CITY1-002 (192.168.21.71)	None	None

2 Enter a new password.

3 Re-enter the password to confirm.

4 Click **OK**. The password has been changed and the dialog closes.



New Password: ****

Confirm Password: ****

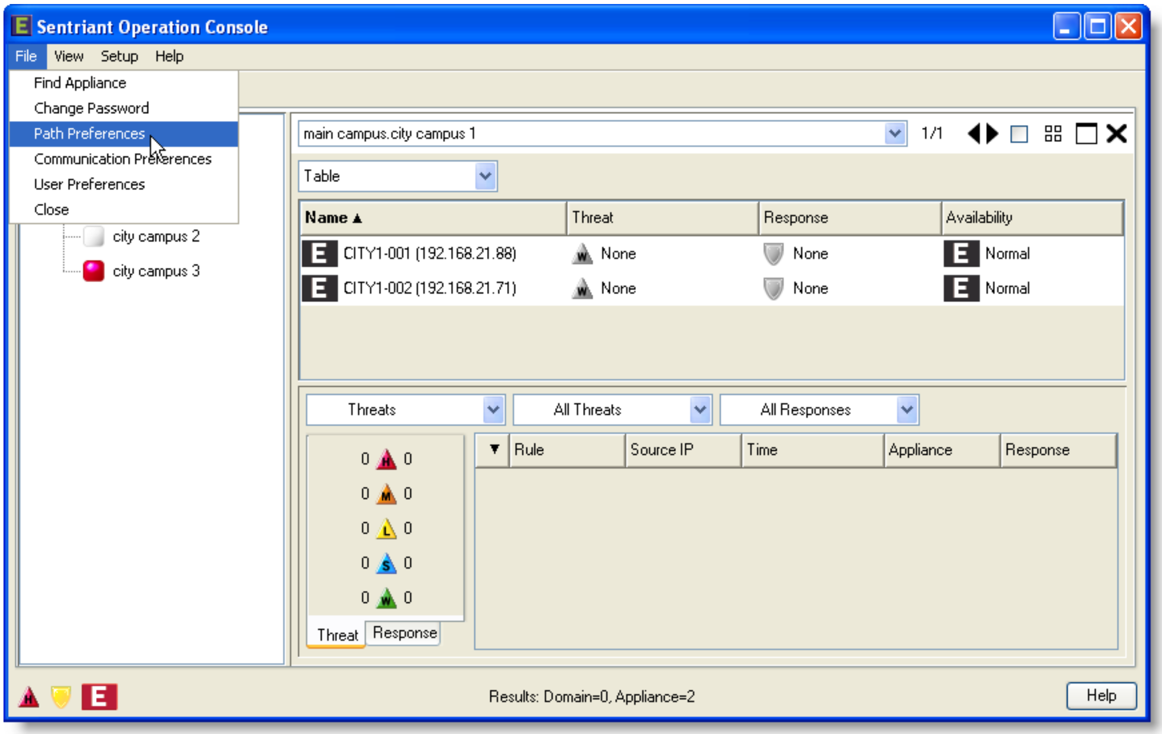
Setting Paths

Upon installation of SOC, default paths are saved for the following components:

- Policy Backup - When performing a policy distribution, a backup is automatically performed in the event of an error. SOC uses this backup to perform a Rollback Policy to the appliance.
- Software Update Cache - The location where downloaded patches are placed.
- Software Update URL - A URL that when updating software, opens an Internet browser displaying available patches for download.
- Sentriant Manager - The location of Sentriant Manager. If Sentriant Manager is uninstalled and reinstalled in a different location, the path should be updated manually.

To set paths:

1 From the Menu, select **File > Path Preferences**.



Name ▲	Threat	Response	Availability
CITY1-001 (192.168.21.88)	None	None	Normal
CITY1-002 (192.168.21.71)	None	None	Normal

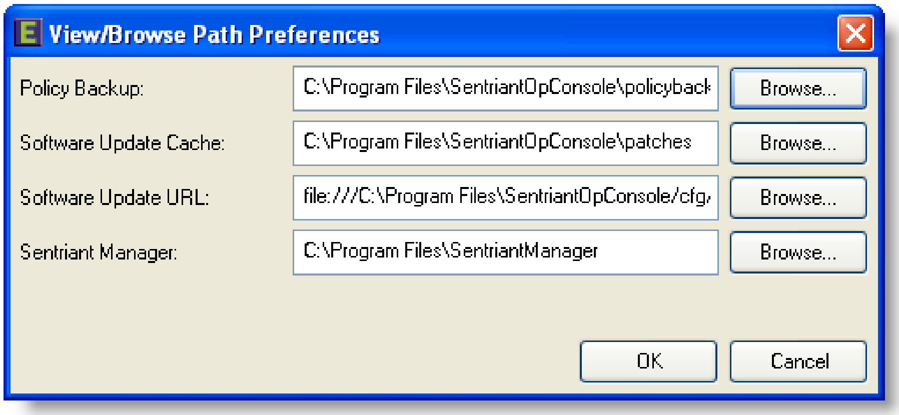
▼	Rule	Source IP	Time	Appliance	Response

Results: Domain=0, Appliance=2

The Path Preferences dialup opens.

2 Click the **Browse** button on the desired path to edit.

3 Click **OK** to save the path changes and close the dialog.



Policy Backup: C:\Program Files\SentriantOpConsole\policyback

Software Update Cache: C:\Program Files\SentriantOpConsole\patches

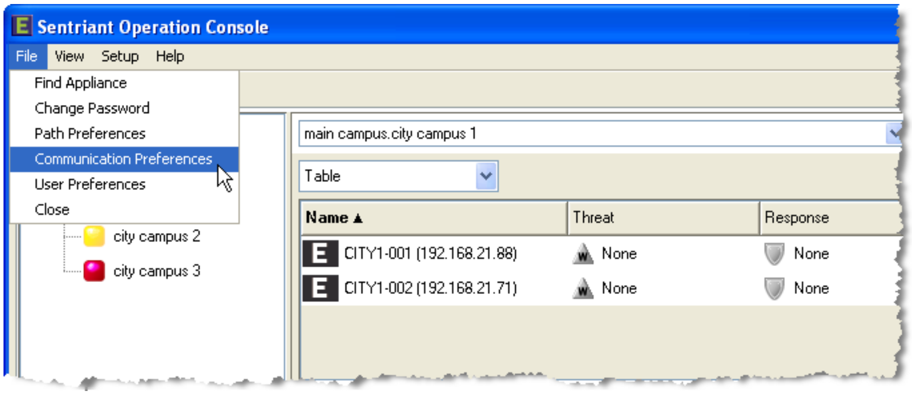
Software Update URL: file:///C:\Program Files\SentriantOpConsole/cfg/

Sentriant Manager: C:\Program Files\SentriantManager

Setting Communication Preferences

To set communication preferences:

1 From the Menu, select **File > Communication Preferences**.

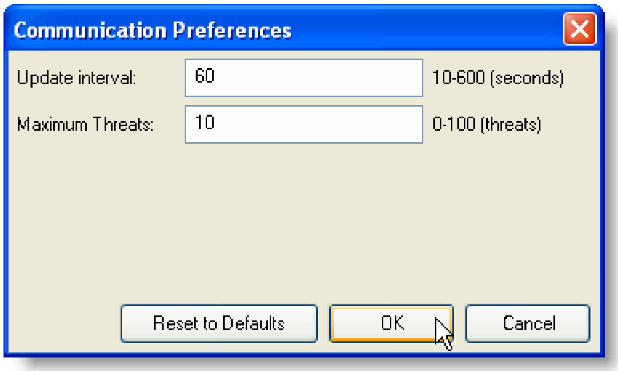


Name ▲	Threat	Response
CITY1-001 (192.168.21.88)	None	None
CITY1-002 (192.168.21.71)	None	None

The Communication Preferences dialog is displayed. It contains values for Update interval and Maximum Threats displayed in the Details Information list. The update interval refreshes threats and is defaulted to update every sixty(60) seconds. The maximum threats displayed is set to ten(10).

2 Enter new values for counter, threat and maximum threats.

3 Click **OK** to accept the changes and close the dialog.



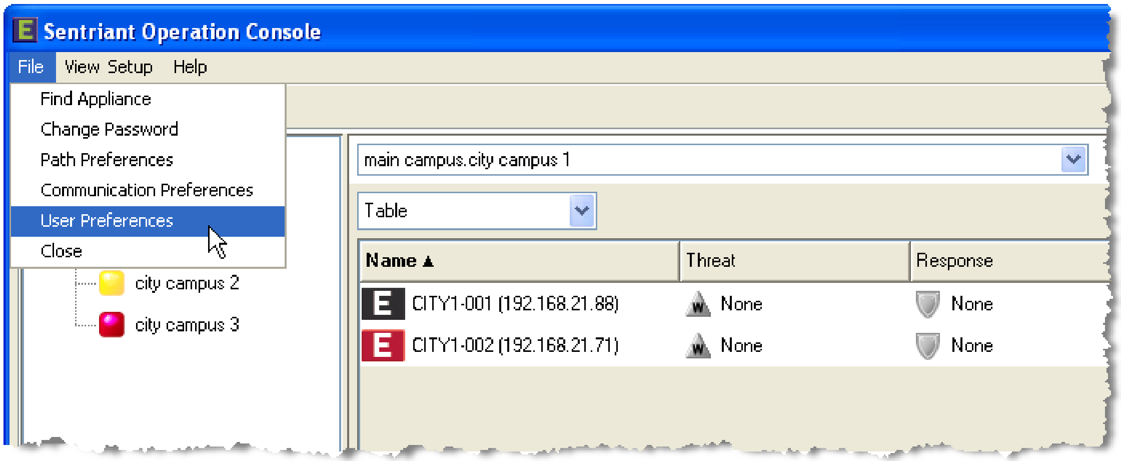
Update interval: 60 10-600 (seconds)

Maximum Threats: 10 0-100 (threats)

Setting User Preferences

To set user preferences:

1 From the Menu, select **File > User Preferences**.



main campus.city campus 1

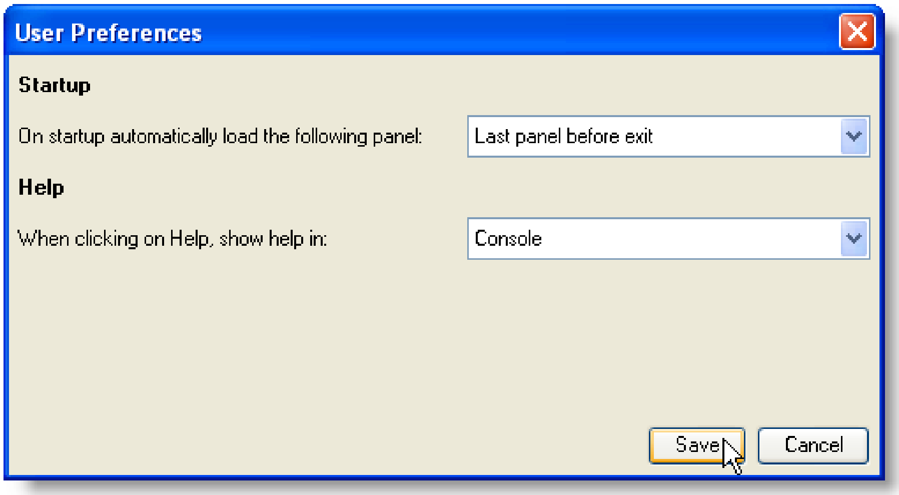
Table

Name ▲	Threat	Response
E CITY1-001 (192.168.21.88)	None	None
E CITY1-002 (192.168.21.71)	None	None

The User Preferences dialog opens. From this dialog, you can change the panel that opens when you start SOC and how the help system is displayed.

2 From the Startup drop-down list, select either Last panel before exit or Use current panel. If you select Last panel before exit, the last panel you had open will reopen the next time you start SOC. If you select Use current panel, the panel you have open when setting this option will open the next time you start SOC.

3 From the Help drop-down list, select either Console, Popup Window, or Help System. Selecting Console will display the console with SOC in the information panel, selecting Popup Window will open a browser-like window, selecting Help System will display help in Java Help application.



Startup

On startup automatically load the following panel: Last panel before exit

Help

When clicking on Help, show help in: Console

3 Setup

The Sentriant Operation Console must be configured to manage appliances. Appliances are added as members of SOC by setting appliance parameters. Once an appliance is a SOC member, the appliance is added to the default domain and is now being monitored.

The SOC gives you the flexibility to group appliances into domains. In an environment where appliances are deployed over a vast geographical area, or in a large deployment where the network is managed by business departments or functions, domains give you the ability to group appliances based on your environment. A domain can be thought of as a folder where appliances are grouped. Domains may also be configured with sub-domains.

The SOC also gives you the ability to share or distribute policy configuration between appliances by loading configuration policy, which was previously saved from a Sentriant. Policy Distribution will load the configuration policy to multiple Sentriants at a time, simplifying the process of sharing policy configuration.

Appliances Panel

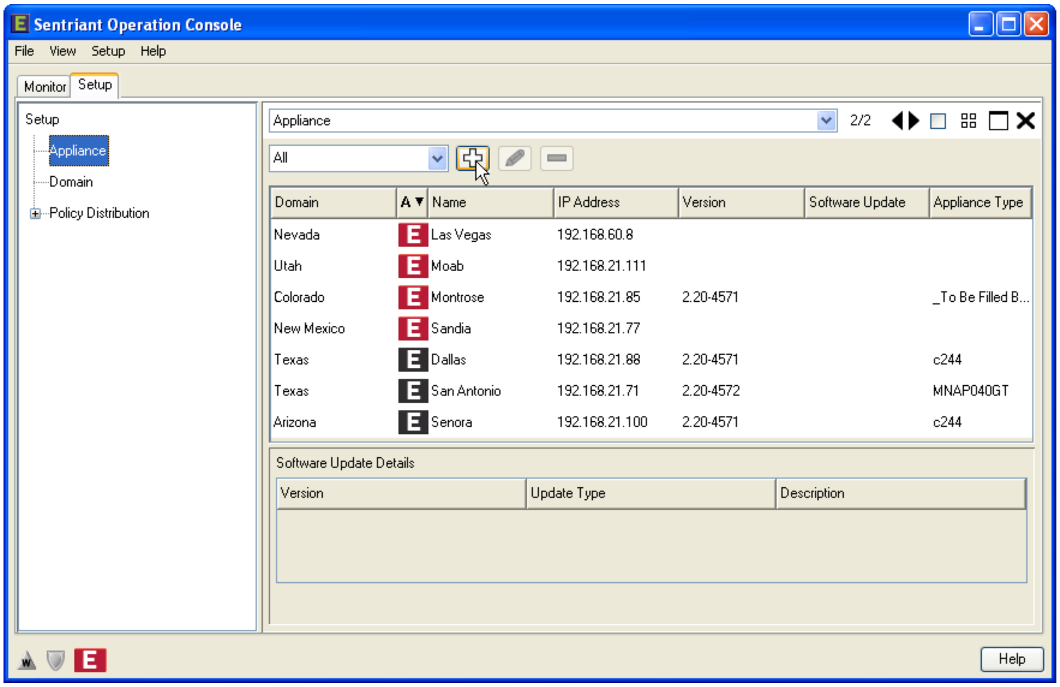
The Appliance Panel is where you will configure and maintain appliances that are members of the SOC. The Appliance Panel consists of an Information Panel and a Software Updates Details Panel. The Information Panel contains appliances that are members of the SOC. Data displayed is the domain where the appliance resides, appliance state, IP Address, software version, software updates, and type. The Software Updates Details Panel displays data for the selected appliance consisting of available software updates, the type of update, and a description of the update.

Adding Appliances

To add an appliance:

1 From the Setup Tab select **Appliance**.

2 Click the **Add Appliance** button.



Domain	A ▼	Name	IP Address	Version	Software Update	Appliance Type
Nevada	E	Las Vegas	192.168.60.8			
Utah	E	Moab	192.168.21.111			
Colorado	E	Montrose	192.168.21.85	2.20-4571		_To Be Filled B...
New Mexico	E	Sandia	192.168.21.77			
Texas	E	Dallas	192.168.21.88	2.20-4571		c244
Texas	E	San Antonio	192.168.21.71	2.20-4572		MNAP040GT
Arizona	E	Senora	192.168.21.100	2.20-4571		c244

Software Update Details

Version	Update Type	Description

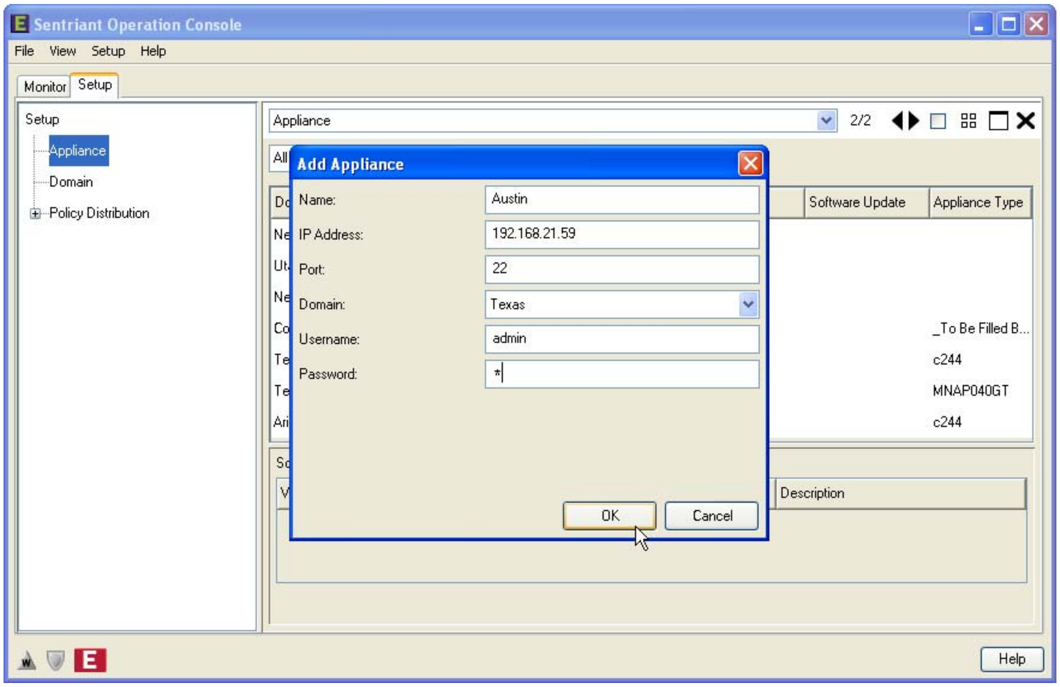
3 Enter the name and IP Address of the appliance. If you have created domains, you may select a domain from the drop-down list. If no domains have been created, the appliance will be placed in the default domain.

NOTE

The Port field is default to 22. If your workstation is configured in a Network Access Translation environment (NAT), you will need to enter the NAT access port number in Port field when adding an appliance and point to port 22 in the NAT access point.

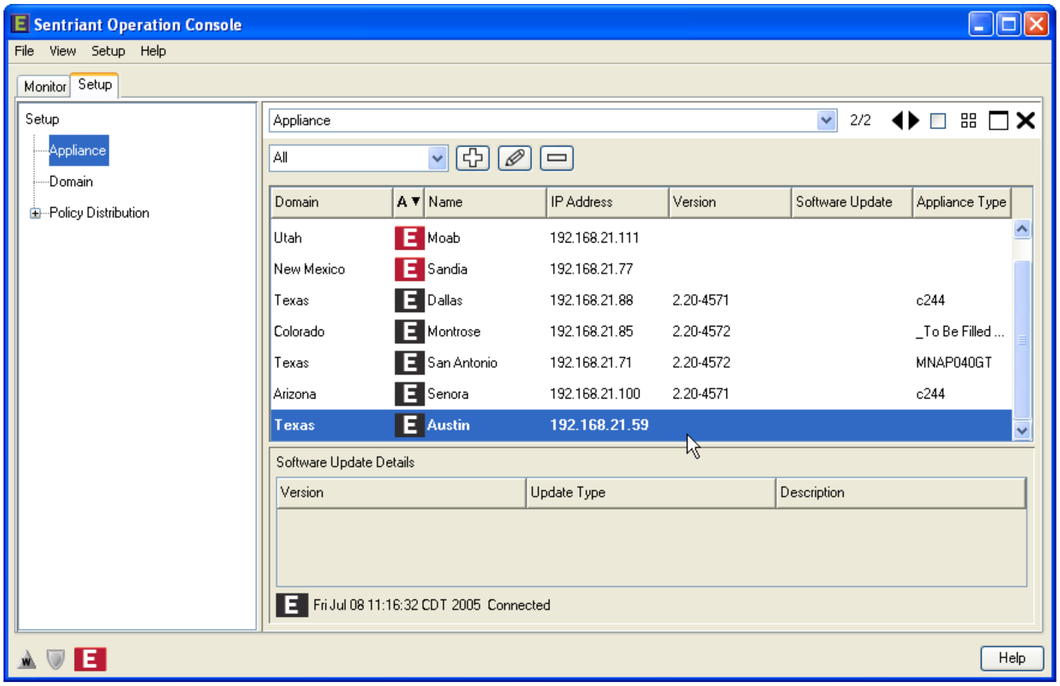
4 Enter the username and password.

5 Click **OK.**



Name: Austin
IP Address: 192.168.21.59
Port: 22
Domain: Texas
Username: admin
Password: *

The appliance is added as a member of SOC.



Domain	A ▼	Name	IP Address	Version	Software Update	Appliance Type
Utah	E	Moab	192.168.21.111			
New Mexico	E	Sandia	192.168.21.77			
Texas	E	Dallas	192.168.21.88	2.20-4571		c244
Colorado	E	Montrose	192.168.21.85	2.20-4572		_To Be Filled ...
Texas	E	San Antonio	192.168.21.71	2.20-4572		MNAP040GT
Arizona	E	Senora	192.168.21.100	2.20-4571		c244
Texas	E	Austin	192.168.21.59			

Version	Update Type	Description

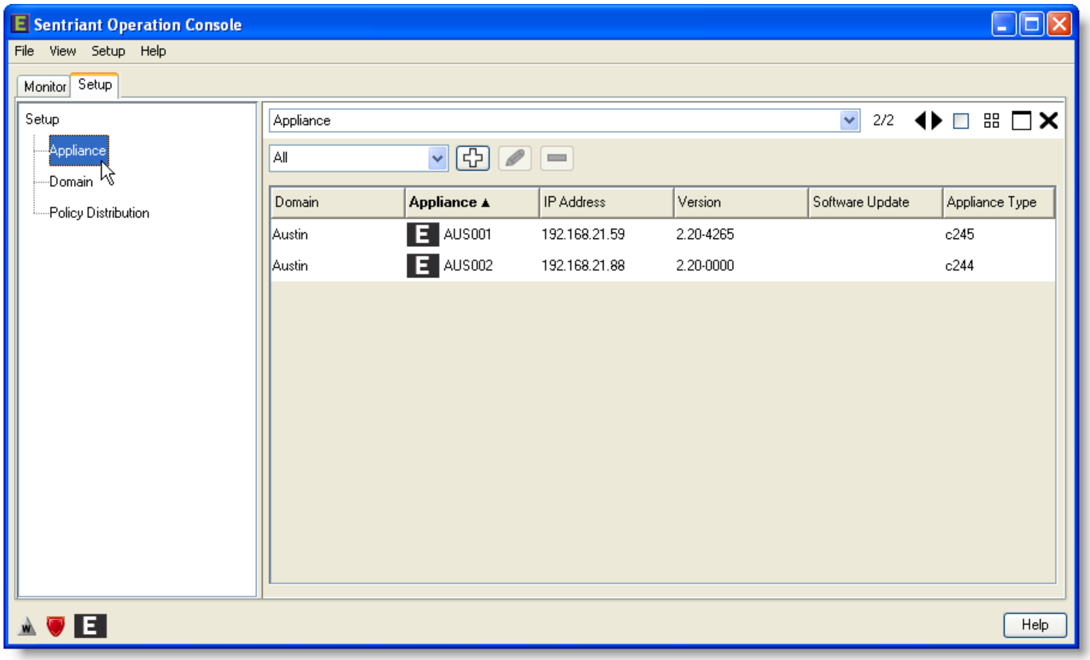
Fri Jul 08 11:16:32 CDT 2005 Connected

View Appliance Information

The **Setup Panel** provides a list of appliances that are SOC members. Selecting an individual appliance provides additional details.

To display information about an appliance:

1 From the Setup tab, click **Appliance**.



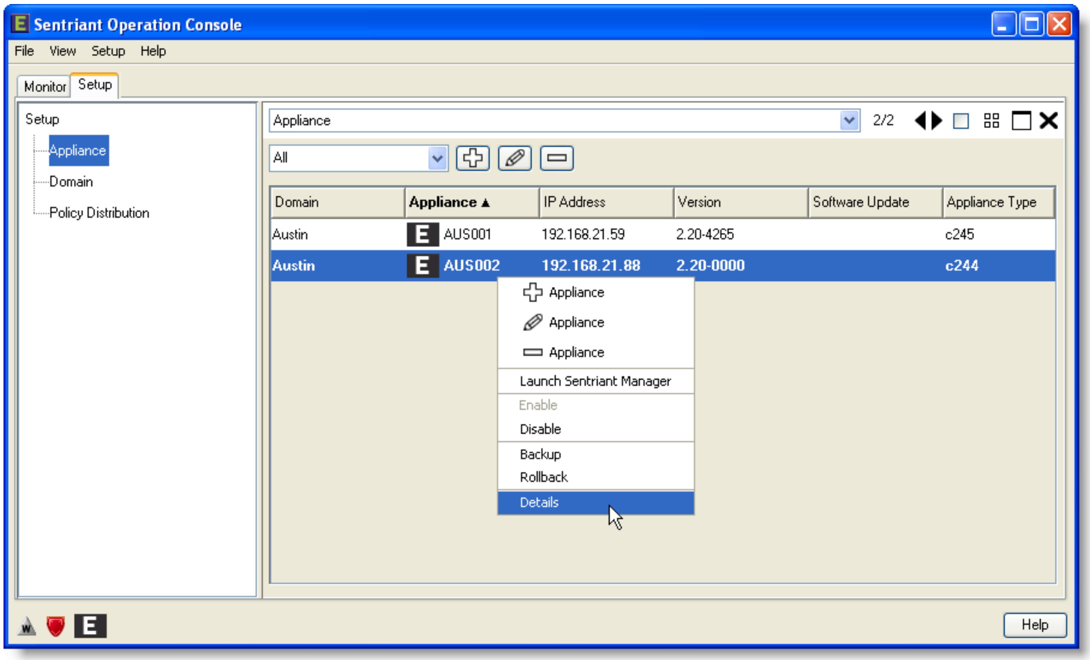
Domain	Appliance ▲	IP Address	Version	Software Update	Appliance Type
Austin	AUS001	192.168.21.59	2.20-4265		c245
Austin	AUS002	192.168.21.88	2.20-0000		c244

The Appliance Panel opens and displays appliance that are members of the SOC. Appliance parameters are displayed in the information panel for the following:

- Domain - the domain where the appliance resides
- Availability - the status of the appliance
- Name - the appliance name
- IP Address - the IP Address of the appliance
- Version - the version number of the Sentriant software
- Software Update - the version number of available Sentriant software updates
- Appliance Type - the model number of the Sentriant appliance

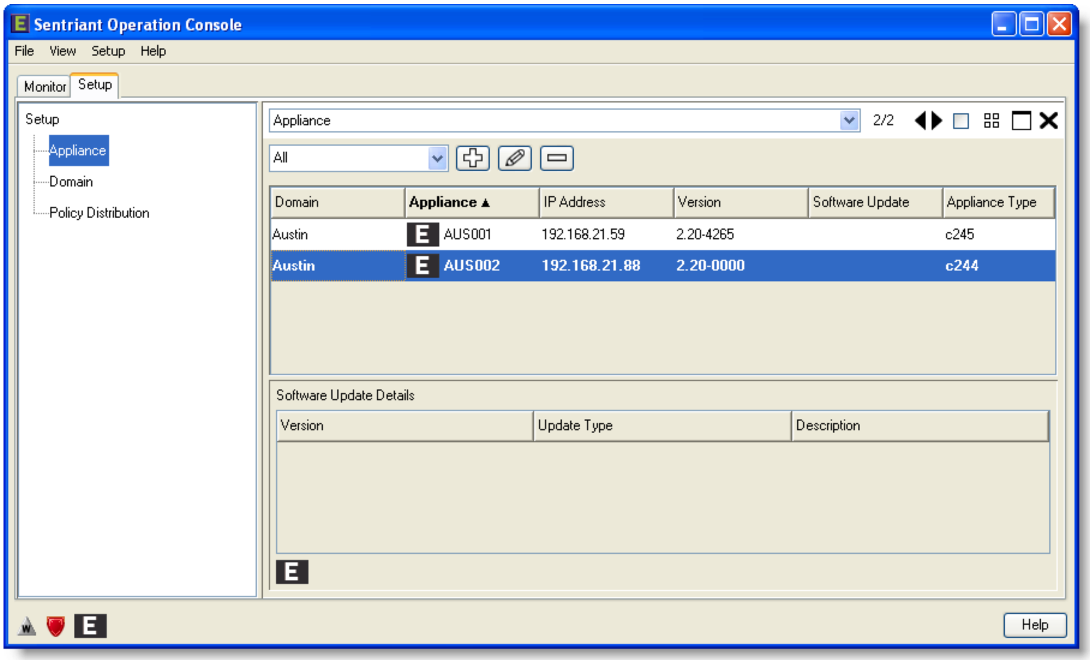
To view appliance details:

1 Double-click on an appliance or right-click and select **Details**.



Domain	Appliance ▲	IP Address	Version	Software Update	Appliance Type
Austin	AUS001	192.168.21.59	2.20-4265		c245
Austin	AUS002	192.168.21.88	2.20-0000		c244

The Software Update Details panel opens that displays software updates available for appliances.



Domain	Appliance ▲	IP Address	Version	Software Update	Appliance Type
Austin	AUS001	192.168.21.59	2.20-4265		c245
Austin	AUS002	192.168.21.88	2.20-0000		c244

Software Update Details

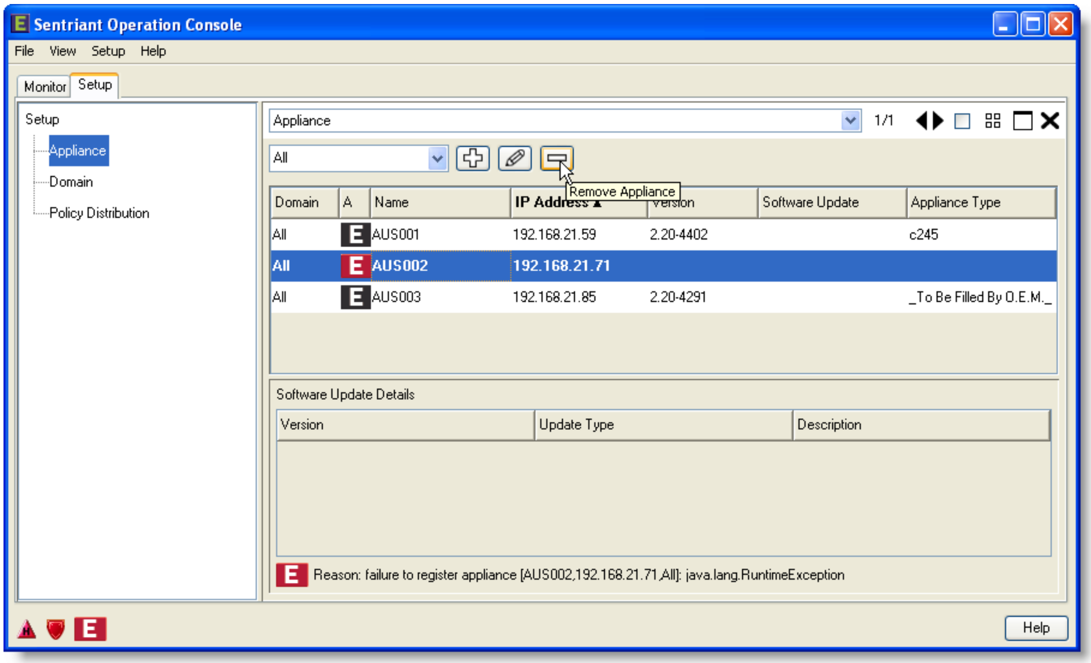
Version	Update Type	Description

Removing Appliances

To remove appliances from SOC:

1 From the Setup Tab, select **Appliance**.

2 Click the **Remove Appliance** button or right-click and select Remove Appliance.



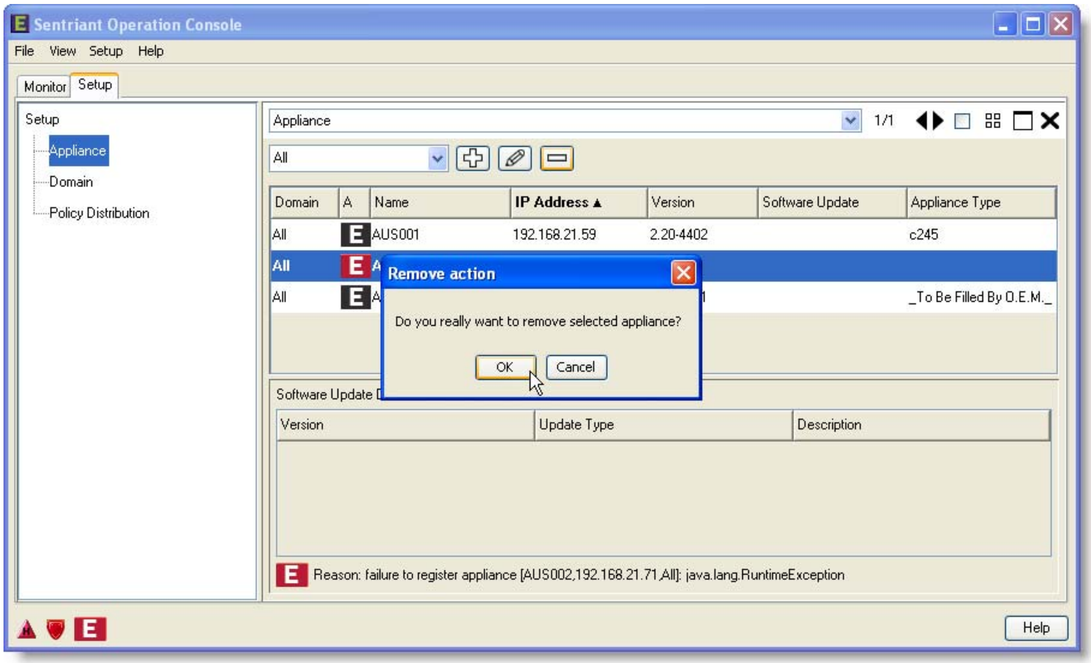
Domain	A	Name	IP Address ▲	Version	Software Update	Appliance Type
All	E	AUS001	192.168.21.59	2.20-4402		c245
All	E	AUS002	192.168.21.71			
All	E	AUS003	192.168.21.85	2.20-4291		_To Be Filled By O.E.M._

Software Update Details

Version	Update Type	Description

Reason: failure to register appliance [AUS002,192.168.21.71,All]: java.lang.RuntimeException

3 Click **OK**.



Domain	A	Name	IP Address ▲	Version	Software Update	Appliance Type
All	E	AUS001	192.168.21.59	2.20-4402		c245
All	E	A				
All	E	A		1		_To Be Filled By O.E.M._

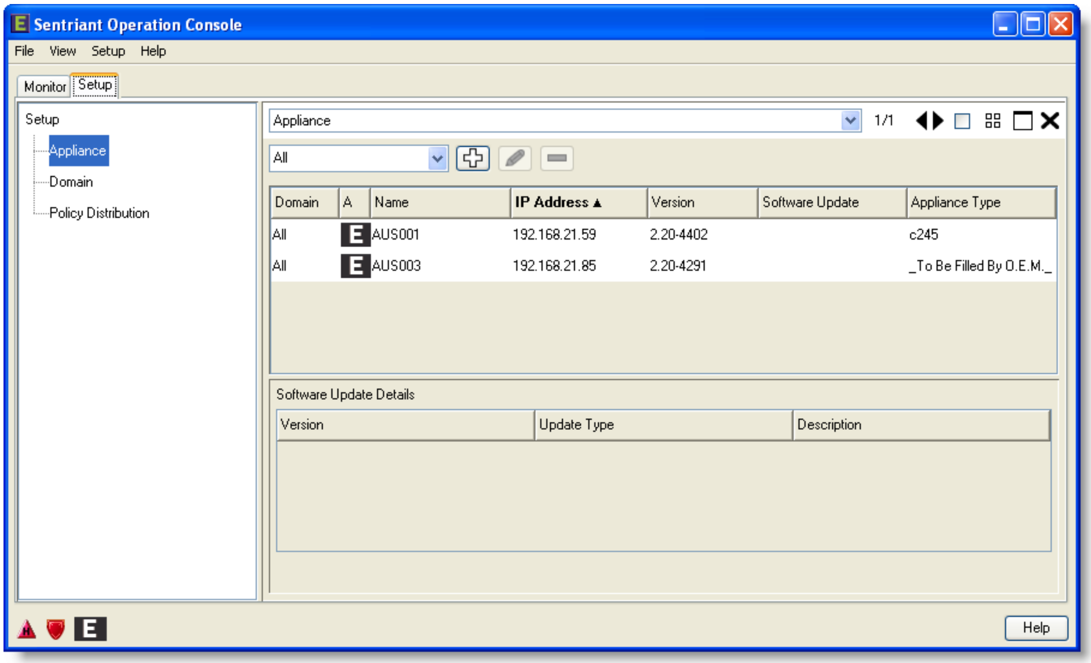
Do you really want to remove selected appliance?

Software Update D

Version	Update Type	Description

Reason: failure to register appliance [AUS002,192.168.21.71,All]: java.lang.RuntimeException

The appliance is removed from SOC.



Domain	A	Name	IP Address ▲	Version	Software Update	Appliance Type
All	E	AUS001	192.168.21.59	2.20-4402		c245
All	E	AUS003	192.168.21.85	2.20-4291		_To Be Filled By O.E.M._

Software Update Details

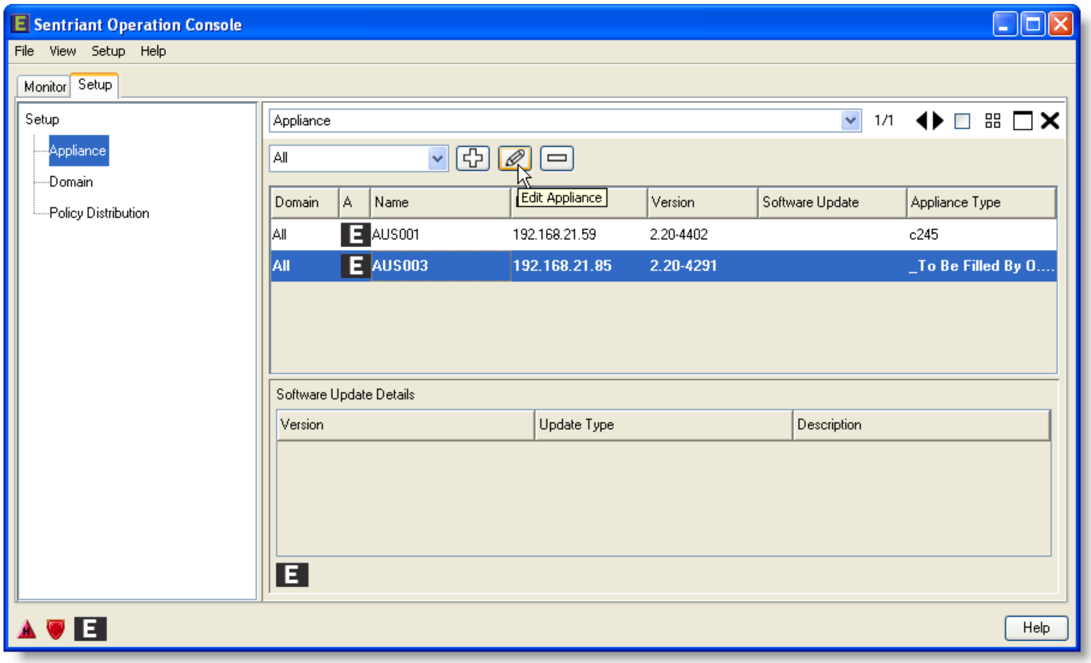
Version	Update Type	Description

Editing Appliances

To edit an appliance from SOC:

1 From the Setup Tab, select **Appliance**.

2 Click the **Edit Appliance** button or right-click and select Edit Appliance.



Domain	A	Name		Version	Software Update	Appliance Type
All	E	AUS001	192.168.21.59	2.20-4402		c245
All	E	AUS003	192.168.21.85	2.20-4291		_To Be Filled By O....

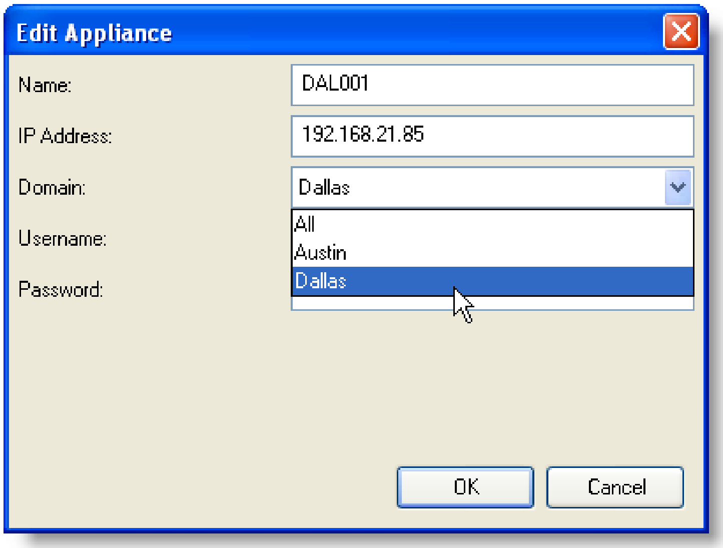
Software Update Details

Version	Update Type	Description

The Edit Appliance dialog opens.

3 Edit the Name, IP Address as necessary.

4 If moving the appliance to another domain, select the domain from the drop-down list.



Edit Appliance

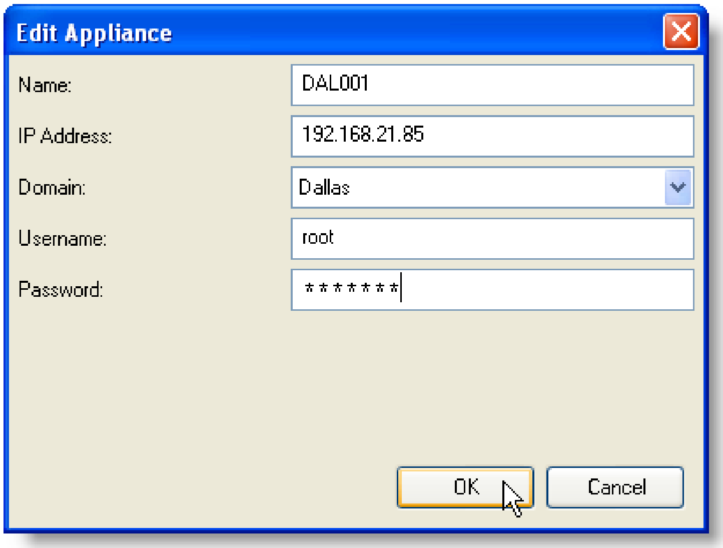
Name: DAL001

IP Address: 192.168.21.85

Domain: Dallas

5 Edit the Username and password.

6 Click **OK**.



Edit Appliance

Name: DAL001

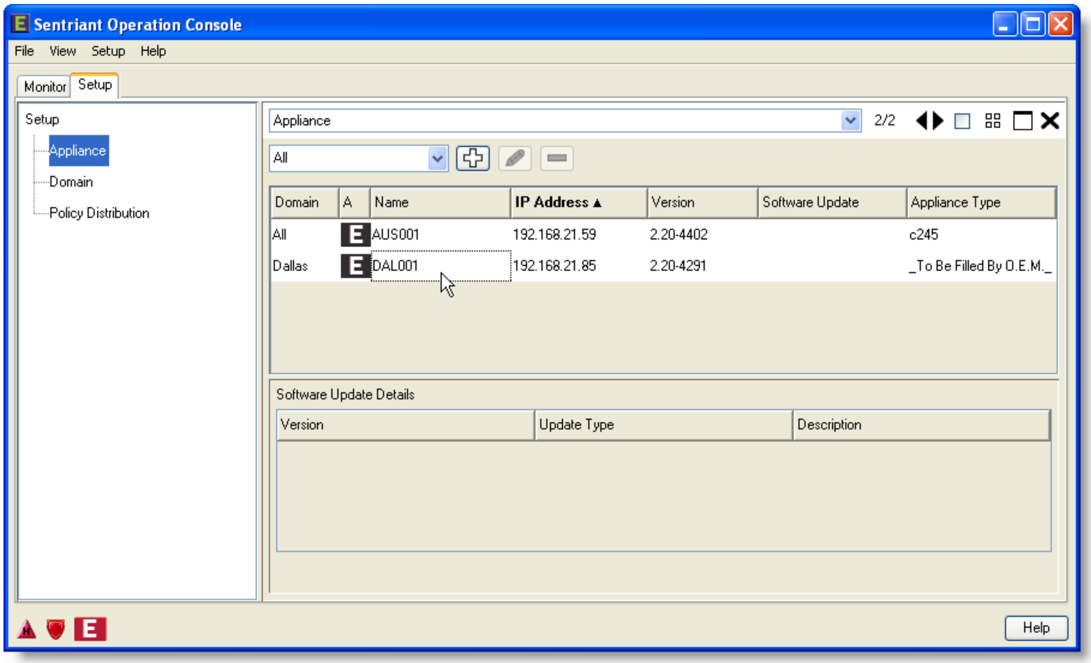
IP Address: 192.168.21.85

Domain: Dallas

Username: root

Password: *******

The appliance is updated with the new parameters.



Domain	A	Name	IP Address ▲	Version	Software Update	Appliance Type
All	E	AUS001	192.168.21.59	2.20-4402		c245
Dallas	E	DAL001	192.168.21.85	2.20-4291		_To Be Filled By O.E.M._

Software Update Details

Version	Update Type	Description

Appliance Software Updates

NOTE

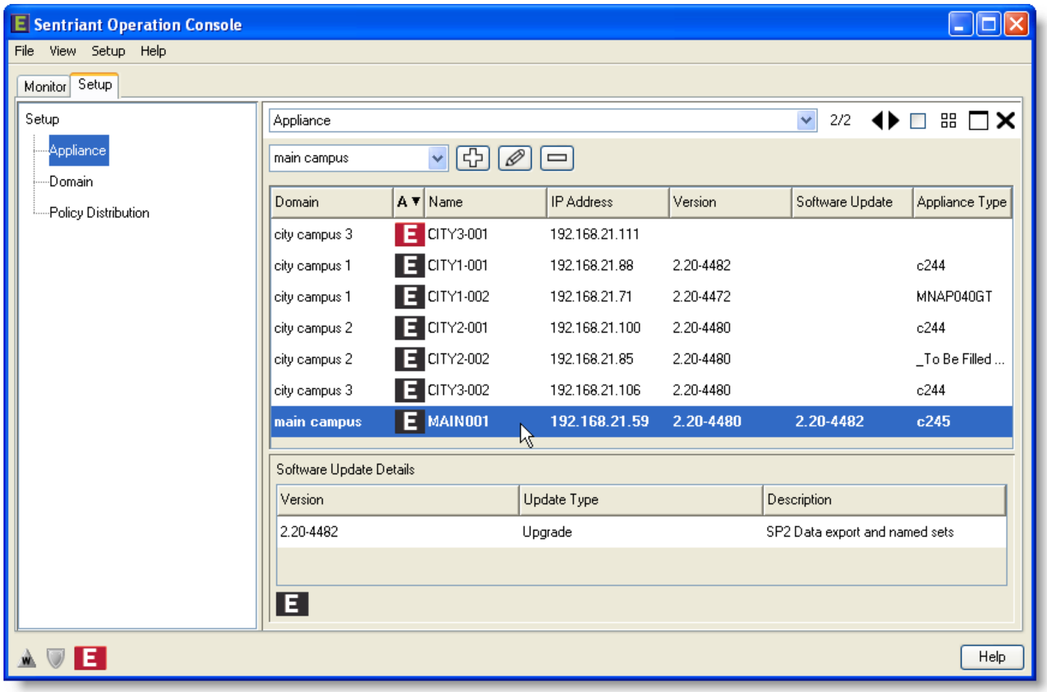
The appliance software update feature is not implemented at this time. The below procedures are for reference only. The appliance software update feature will be implemented in a later version of the software.

Sentriant appliance software updates can be performed from SOC. Available software updates are listed in the Software Update Details panel and in the Software Updates column. The list contains the version number of the update, the type of update and a description. Selecting an update will start the download and patching process to the appliance. Only valid patches will be displayed in the list based on the type of appliance.

To view available software updates:

1 From the Setup Tab, click **Appliance** from the list on the left of the screen.

2 Locate and select an appliance to update.



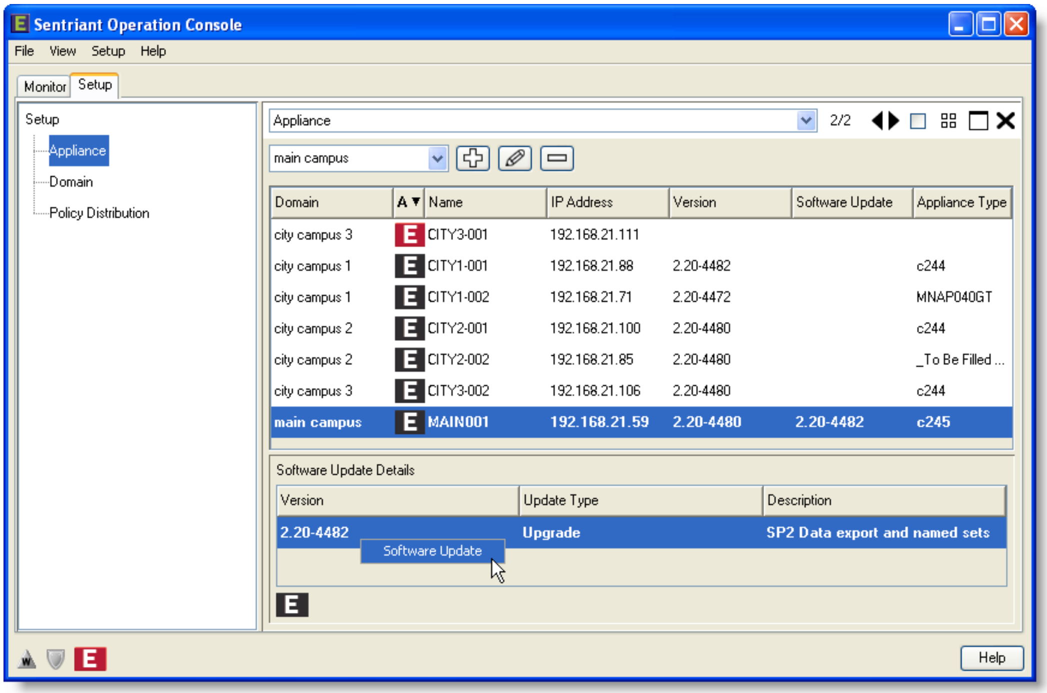
Domain	A ▾	Name	IP Address	Version	Software Update	Appliance Type
city campus 3	E	CITY3-001	192.168.21.111			
city campus 1	E	CITY1-001	192.168.21.88	2.20-4482		c244
city campus 1	E	CITY1-002	192.168.21.71	2.20-4472		MNAP040GT
city campus 2	E	CITY2-001	192.168.21.100	2.20-4480		c244
city campus 2	E	CITY2-002	192.168.21.85	2.20-4480		_To Be Filled ...
city campus 3	E	CITY3-002	192.168.21.106	2.20-4480		c244
main campus	E	MAIN001	192.168.21.59	2.20-4480	2.20-4482	c245

Software Update Details

Version	Update Type	Description
2.20-4482	Upgrade	SP2 Data export and named sets

A list of available software updates is displayed in the Software Update Details panel.

3 Right-click the patch and select **Software Update**.



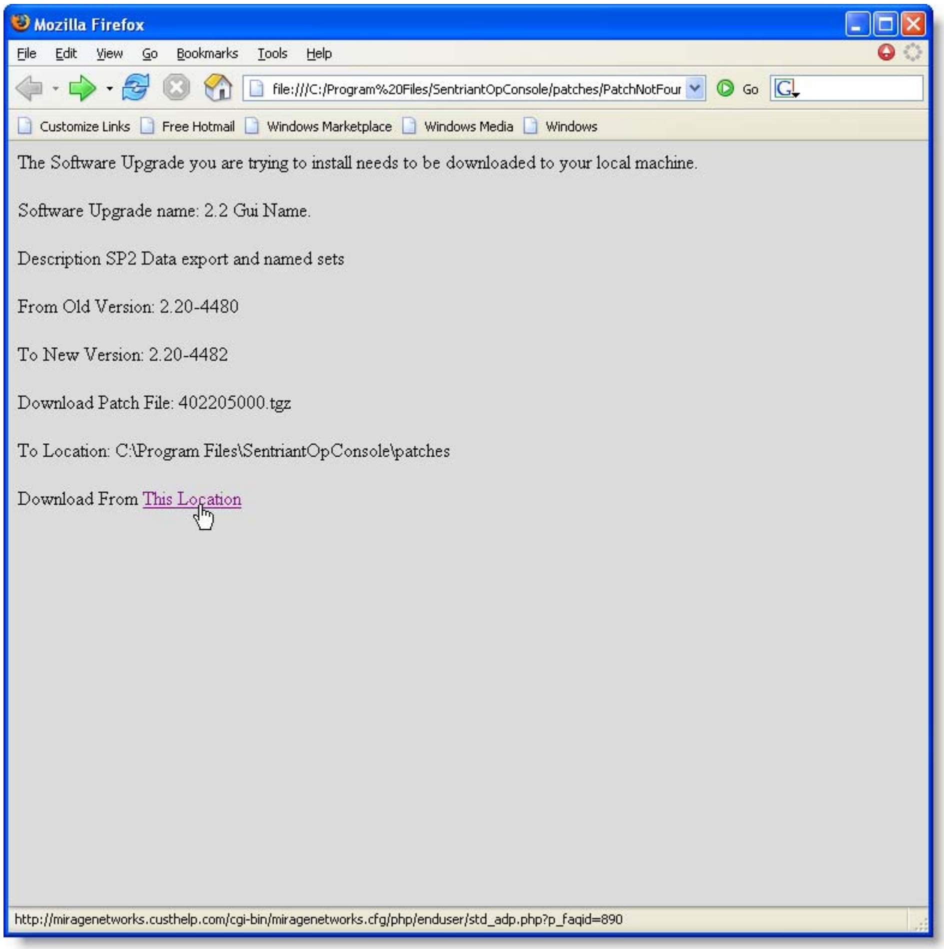
Domain	A ▾	Name	IP Address	Version	Software Update	Appliance Type
city campus 3	E	CITY3-001	192.168.21.111			
city campus 1	E	CITY1-001	192.168.21.88	2.20-4482		c244
city campus 1	E	CITY1-002	192.168.21.71	2.20-4472		MNAP040GT
city campus 2	E	CITY2-001	192.168.21.100	2.20-4480		c244
city campus 2	E	CITY2-002	192.168.21.85	2.20-4480		_To Be Filled ...
city campus 3	E	CITY3-002	192.168.21.106	2.20-4480		c244
main campus	E	MAIN001	192.168.21.59	2.20-4480	2.20-4482	c245

Software Update Details

Version	Update Type	Description
2.20-4482	Upgrade	SP2 Data export and named sets

If the patch file has not been found on the local machine in the path set from the Path Preferences, a web browser opens notifying you that the file must be downloaded.

4 Click the Download From This Location link at the bottom of the page.



Mozilla Firefox
File Edit View Go Bookmarks Tools Help
file:///C:/Program%20Files/SentriantOpConsole/patches/PatchNotFour
Go
Customize Links
Free Hotmail
Windows Marketplace
Windows Media
Windows

The Software Upgrade you are trying to install needs to be downloaded to your local machine.

Software Upgrade name: 2.2 Gui Name.

Description SP2 Data export and named sets

From Old Version: 2.20-4480

To New Version: 2.20-4482

Download Patch File: 402205000.tgz

To Location: C:\Program Files\SentriantOpConsole\patches

Download From This Location

http://miragenetworks.custhelp.com/cgi-bin/miragenetworks.cfg/php/enduser/std_adp.php?p_faqid=890

The download process begins by downloading the patch file to the local machine into the path set in the Path Preferences. Once the download has completed, Sentriant Manager is launched and begins the update process.

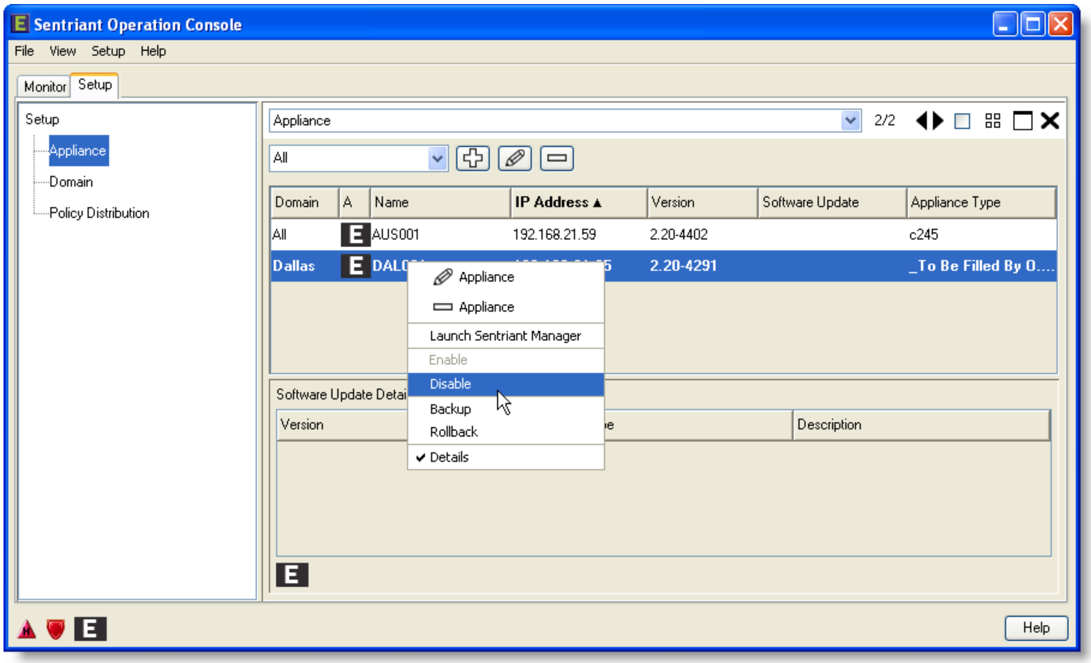
Disable/Enable Appliances

To disable an appliance:

1 From the Setup Tab, select **Appliance**.

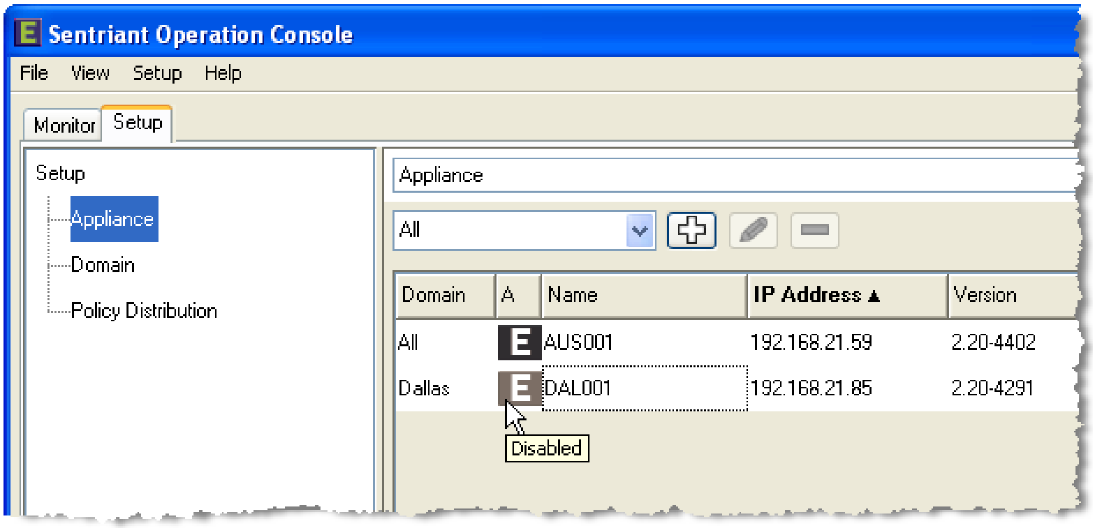
2 Select an appliance.

3 Right-click and select **Disable**.



Domain	A	Name	IP Address ▲	Version	Software Update	Appliance Type
All	E	AUS001	192.168.21.59	2.20-4402		c245
Dallas	E	DAL0	5	2.20-4291		_To Be Filled By O....

The appliance Availability icon will turn gray. The Sentriant continues to detect and mitigate threats but is no longer being monitored by SOC.



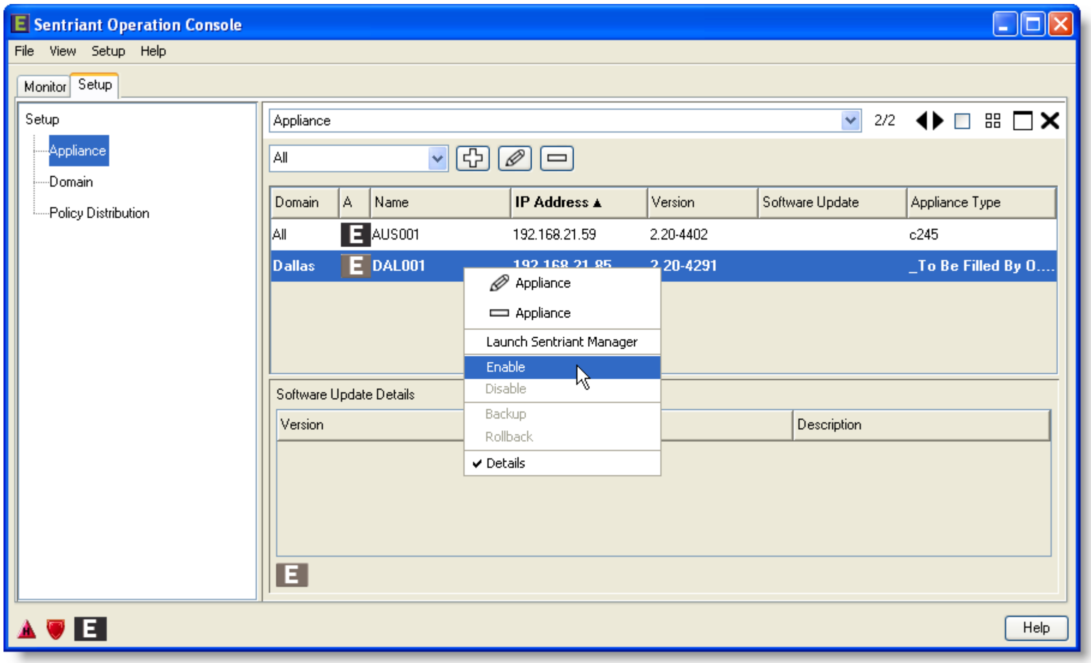
Domain	A	Name	IP Address ▲	Version
All	E	AUS001	192.168.21.59	2.20-4402
Dallas	E	DAL001	192.168.21.85	2.20-4291

To enable an appliance:

1 From the Setup Tab, select **Appliance**.

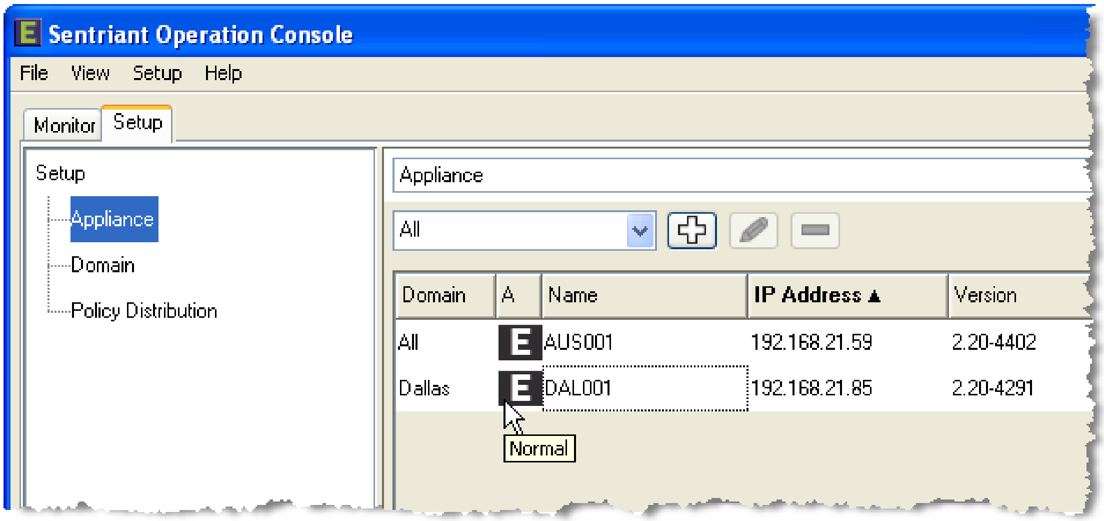
2 Select an appliance.

3 Right-click and select **Enable**.



Domain	A	Name	IP Address ▲	Version	Software Update	Appliance Type
All	E	AUS001	192.168.21.59	2.20-4402		c245
Dallas	E	DAL001	192.168.21.85	2.20-4291		_To Be Filled By O....

The appliance Availability icon will turn black. The appliance now being monitored by SOC.



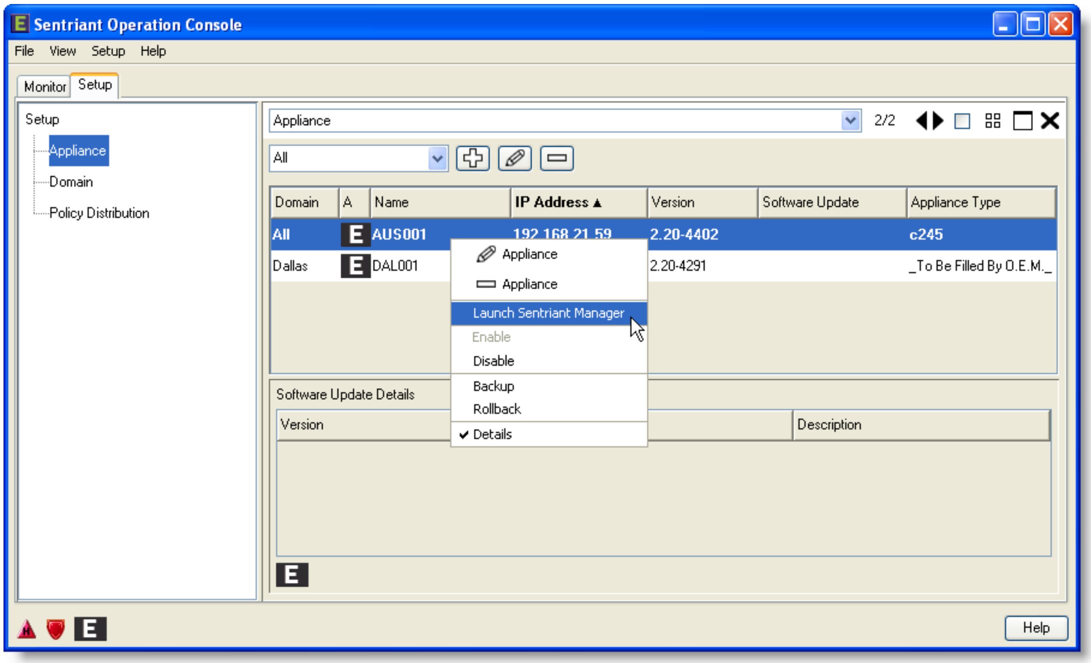
Domain	A	Name	IP Address ▲	Version
All	E	AUS001	192.168.21.59	2.20-4402
Dallas	E	DAL001	192.168.21.85	2.20-4291

Launching Sentriant Manager

To launch Sentriant Manager from SOC:

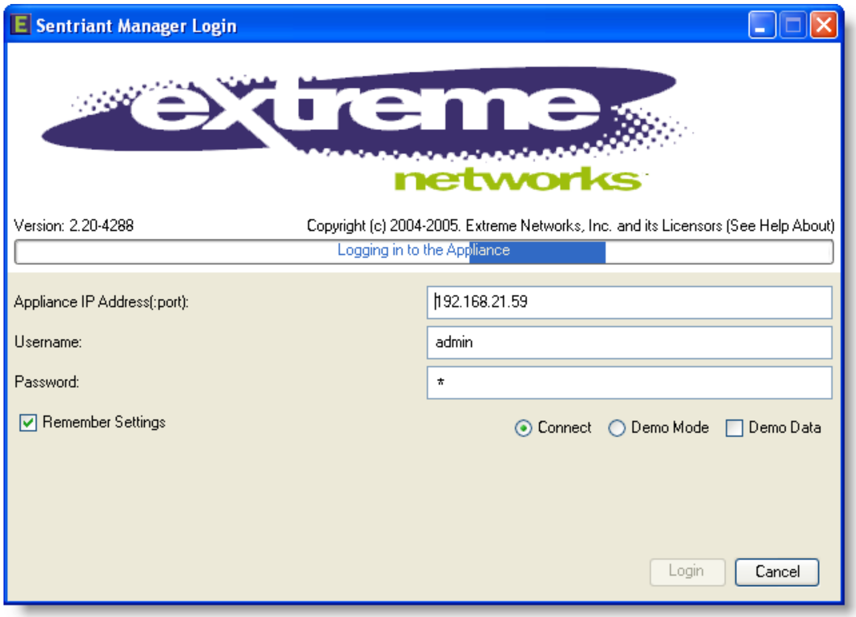
1 From the Setup Tab, select **Appliance**.

2 Right-click an appliance and select **Launch Sentriant Manager**.



Domain	A	Name	IP Address ▲	Version	Software Update	Appliance Type
All	E	AUS001	192.168.21.59	2.20-4402		c245
Dallas	E	DAL001		2.20-4291		_To Be Filled By O.E.M._

The Sentriant Manager Login dialog opens and begins the login process. Note that the appliance parameters have already been populated.



Version: 2.20-4288

Copyright (c) 2004-2005. Extreme Networks, Inc. and its Licensors (See Help About)

Logging in to the Appliance

Appliance IP Address(:port): 192.168.21.59

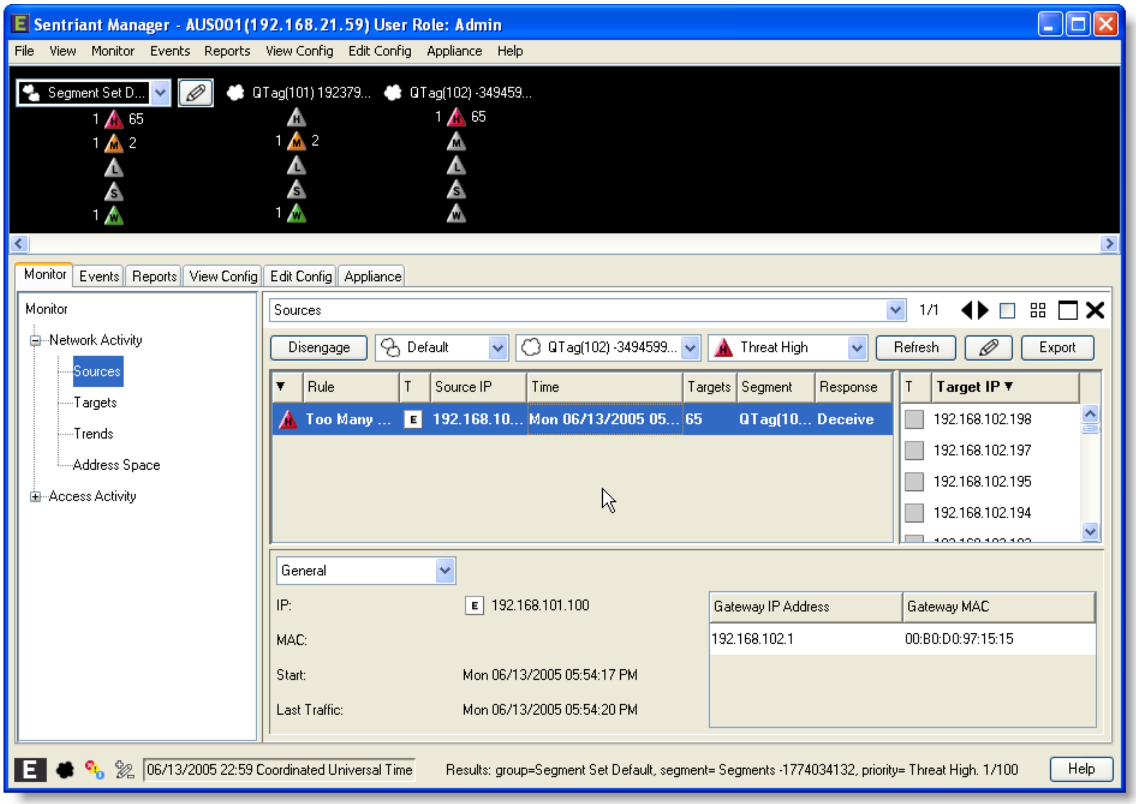
Username: admin

Password: *

☑ Remember Settings

● Connect ○ Demo Mode □ Demo Data

Once the Sentriant Manager is up and running, focus is placed on the panel where you launched Sentriant Manager. In this case, Sentriant Manager was launched from Setup > Appliance. Therefore, Sentriant Manager will open and navigate to the Appliance Panel.



	Rule	T	Source IP	Time	Targets	Segment	Response
▲	Too Many ...	E	192.168.10...	Mon 06/13/2005 05...	65	QTag(10...	Deceive

T	Target IP ▾
□	192.168.102.198
□	192.168.102.197
□	192.168.102.195
□	192.168.102.194

IP: E 192.168.101.100

MAC:

Start: Mon 06/13/2005 05:54:17 PM

Last Traffic: Mon 06/13/2005 05:54:20 PM

Gateway IP Address	Gateway MAC
192.168.102.1	00:B0:D0:97:15:15

06/13/2005 22:59 Coordinated Universal Time

Results: group=Segment Set Default, segment= Segments -1774034132, priority= Threat High. 1/100

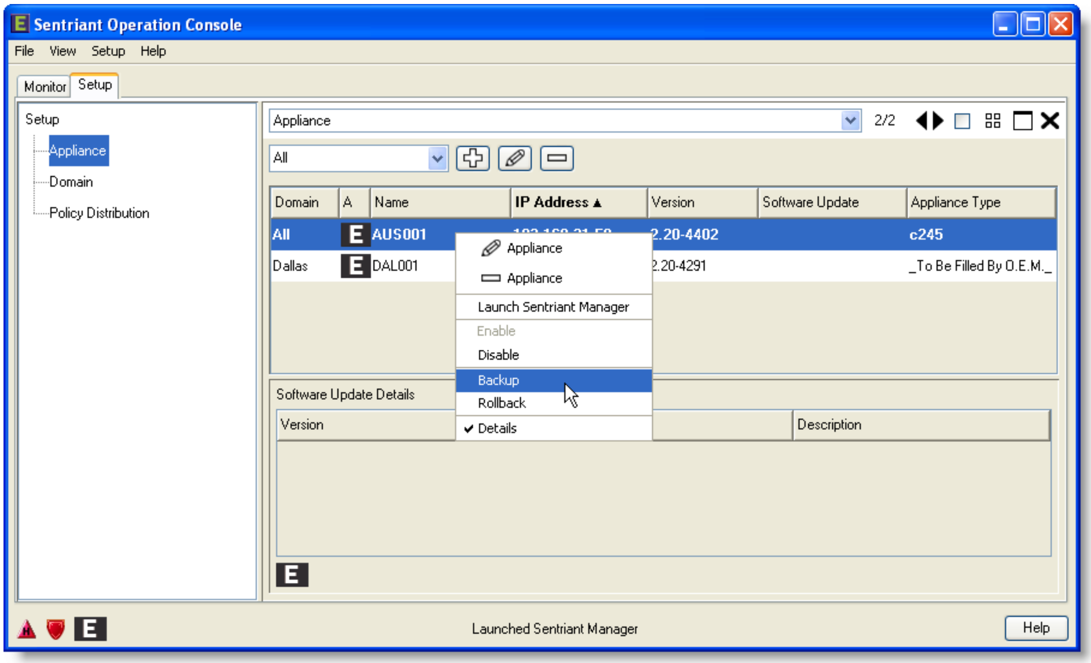
Backup Appliance Configuration

Backup Appliance Configuration is used to save the complete configuration for the selected appliance which includes appliance name, IP Address, user accounts, alerts, deception settings, named items, segment configuration settings, and policy settings. You should backup the appliance anytime you are performing a software update or policy distribution.

To backup an appliance's configuration:

1 From the Setup Tab, select **Appliance**.

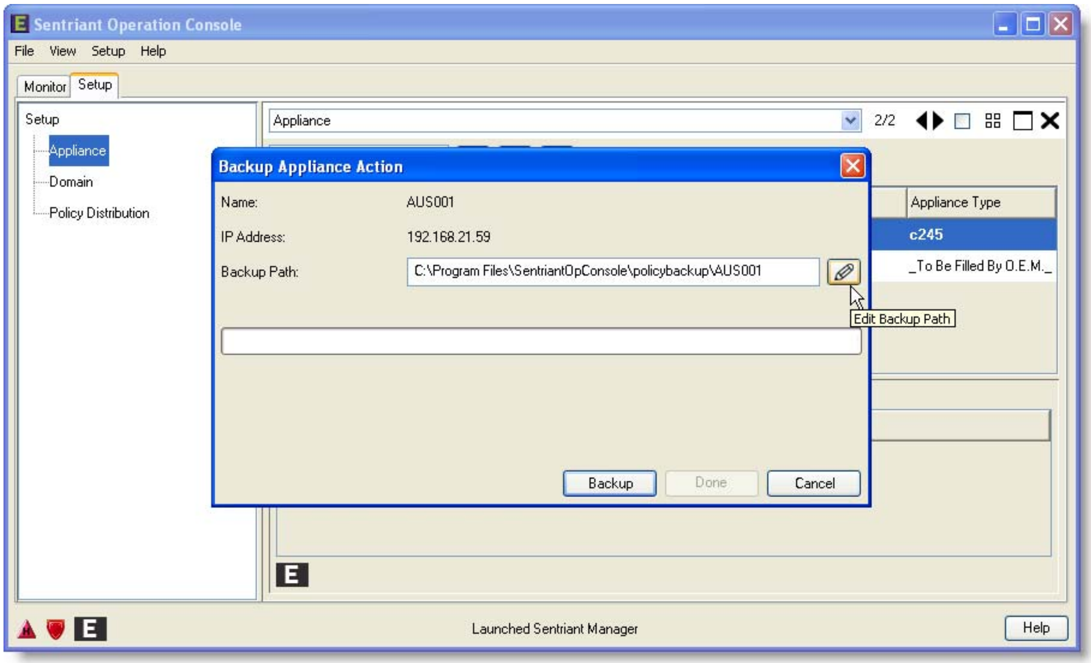
2 Right-click an appliance and select **Backup Configuration**.



Domain	A	Name	IP Address ▲	Version	Software Update	Appliance Type
All	E	AUS001	[illegible]	2.20-4402		c245
Dallas	E	DAL001		2.20-4291		_To Be Filled By O.E.M._

Launched Sentriant Manager

The Backup Appliance Action dialog opens with the default backup path. You may change the path by clicking the **Edit Backup Path** button and entering a new path.



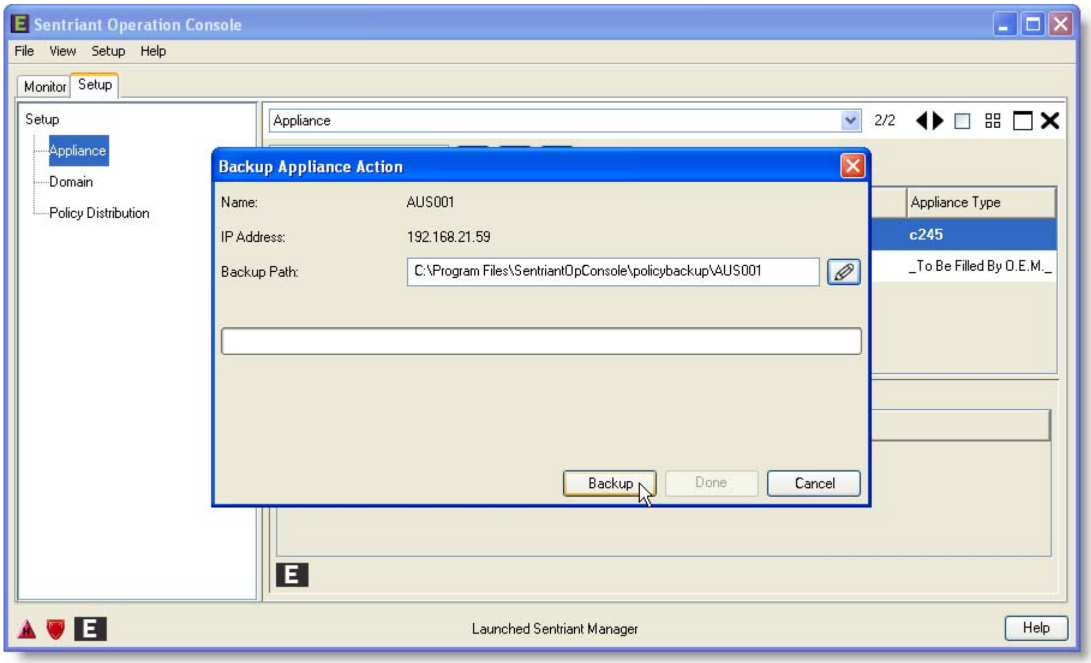
Name: AUS001

IP Address: 192.168.21.59

Backup Path: C:\Program Files\SentriantOpConsole\policybackup\AUS001

Launched Sentriant Manager

3 Click the **Backup** button.



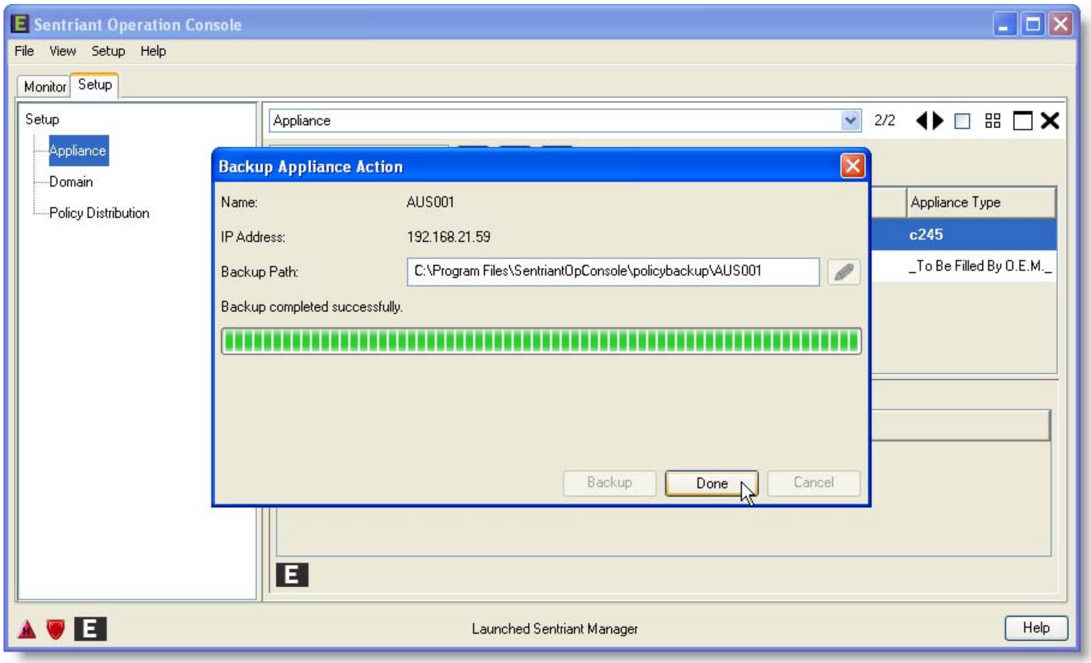
Name: AUS001

IP Address: 192.168.21.59

Backup Path: C:\Program Files\SentriantOpConsole\policybackup\AUS001

Launched Sentriant Manager

A message stating the backup was successful is displayed. Click **Done** to close the dialog and return to SOC.



Backup Appliance Action

Name: AUS001

IP Address: 192.168.21.59

Backup Path: C:\Program Files\SentriantOpConsole\policybackup\AUS001

Backup completed successfully.

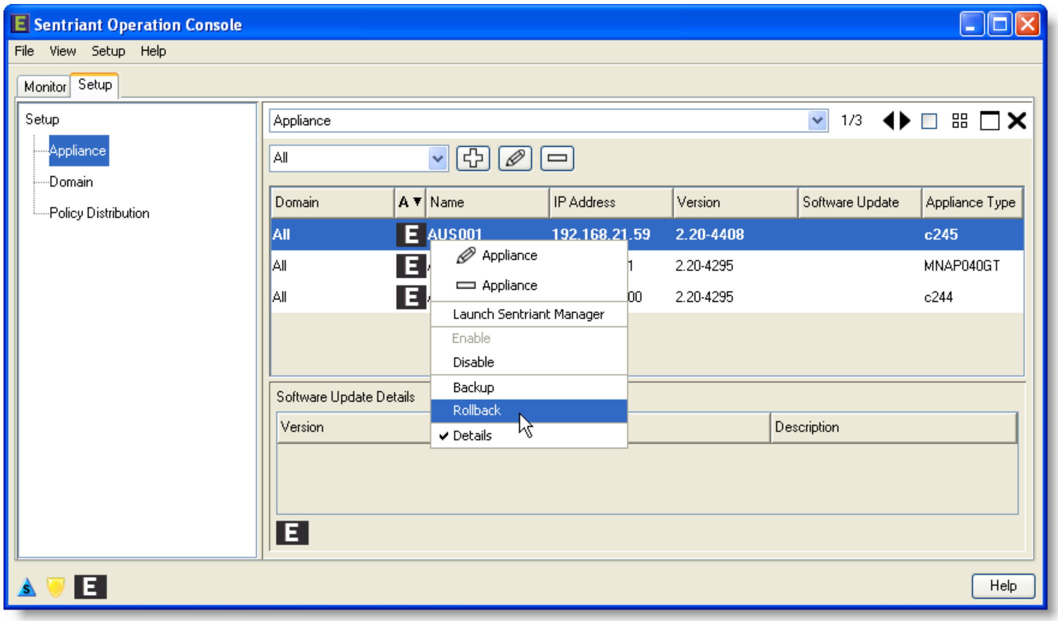
Rollback Policy Distribution

Rollback Policy Distribution is used to reload a saved configuration for the selected appliance which includes appliance name, IP Address, user accounts, alerts, deception settings, named items, segment configuration settings, and policy settings. You should rollback the appliance if an error is encountered with a software update or policy distribution.

To rollback an appliance to the last saved policy distribution:

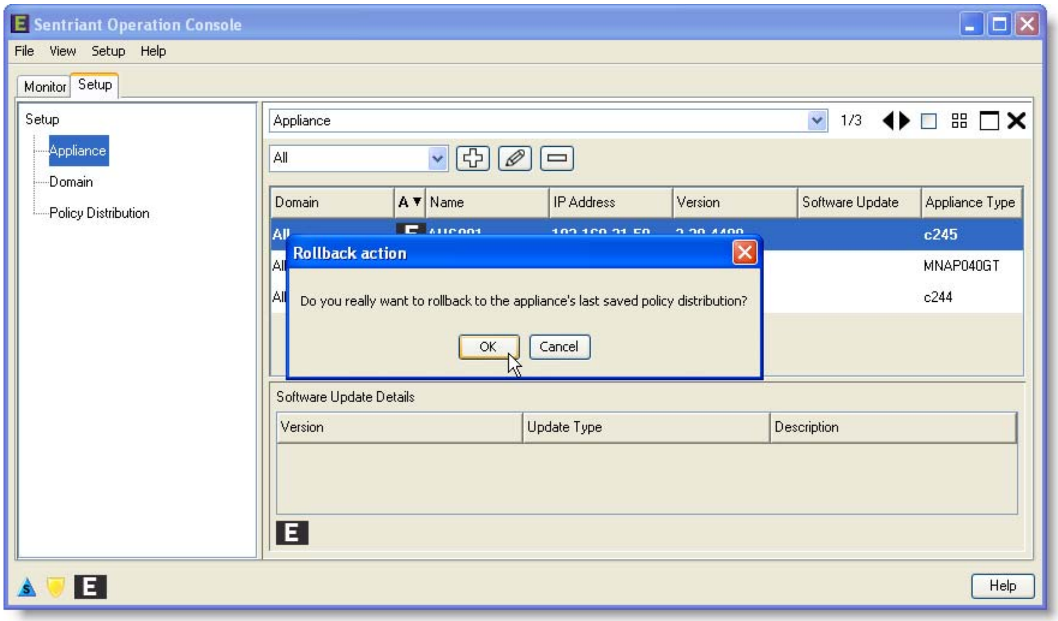
1 From the Setup Tab, select **Appliance**.

2 Right-click an appliance and select **Rollback Policy**.



Domain	A ▼	Name	IP Address	Version	Software Update	Appliance Type
All	E	AUS001	192.168.21.59	2.20-4408		c245
All	E		1	2.20-4295		MNAP040GT
All	E		00	2.20-4295		c244

3 Click **OK** to start rollback.



Rollback action

Do you really want to rollback to the appliance's last saved policy distribution?

Domain Panel

The Domain Panel is where you will configure and maintain domains and appliances that are members of the SOC.

The SOC gives you the flexibility to group appliances into domains. In an environment where appliances are deployed over a vast geographical area, or in a large deployment where the network is managed by business departments or functions, domains give you the ability to group appliances based on your environment.

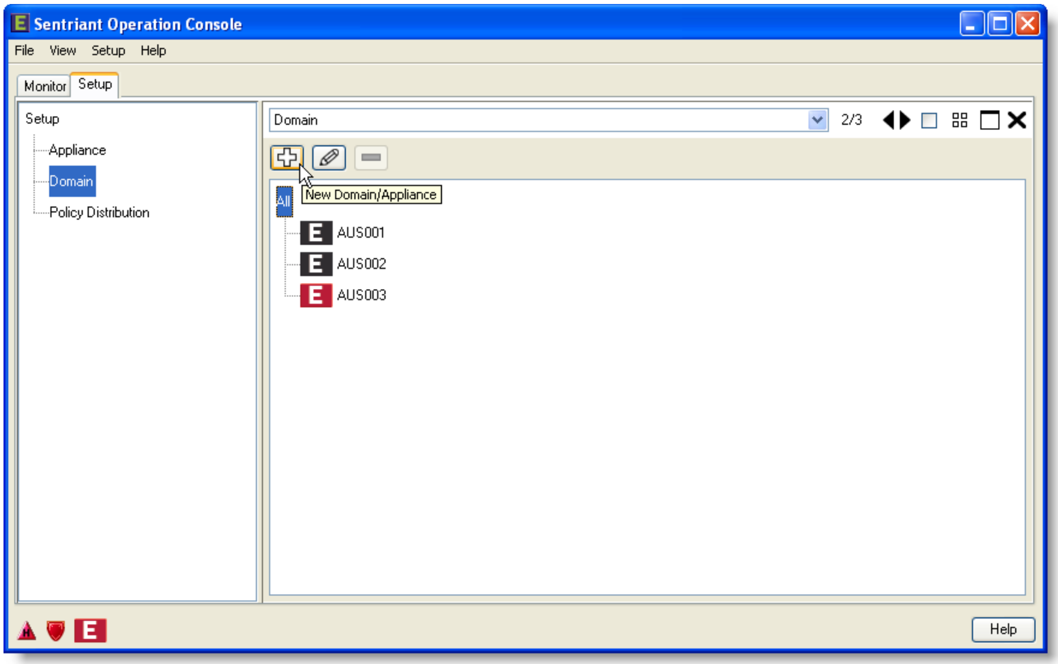
The Domain Panel consists of an Information Panel where you create domains and add or move appliances. When an appliance is added as a member to SOC, it is initially placed in a default domain named All if no other domains have been created or the user does not select a domain while adding the appliance. Domains can be nested within other domains. For example, a network environment is spread out across multiple campuses with a main campus and four campus buildings. A Domain structure would have the main campus at level one and then the four campuses at level two. SOC has no limit on the number of domain levels that may be created.

Creating Domains

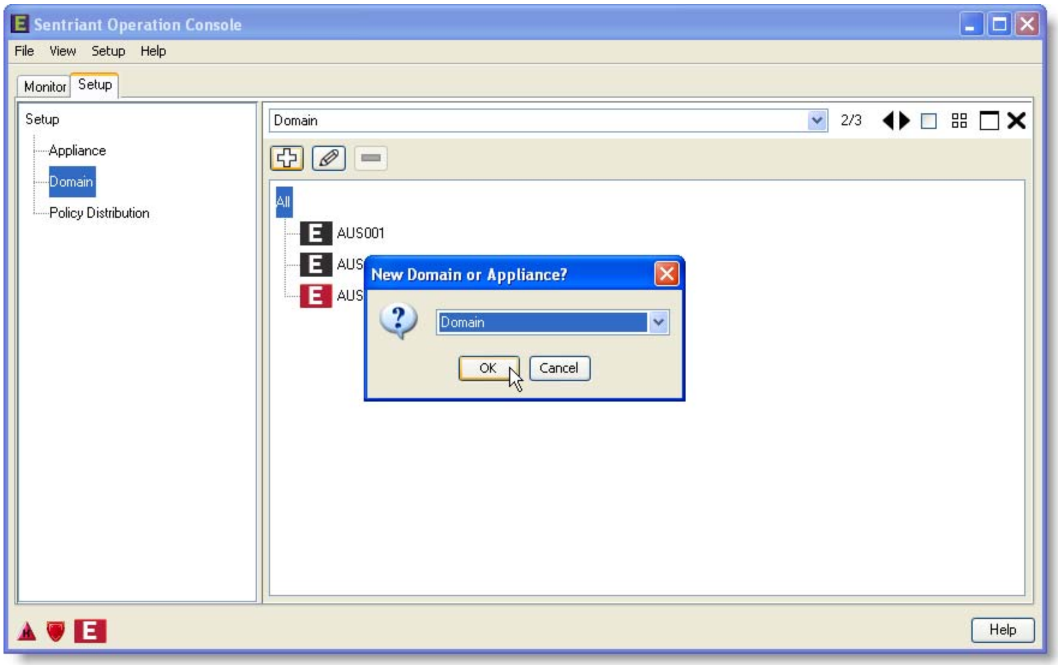
To create domains:

1 From the Setup Tab select **Domain**.

2 Click the **New Domain/Appliance** button or right-click on a domain and select Add Domain.



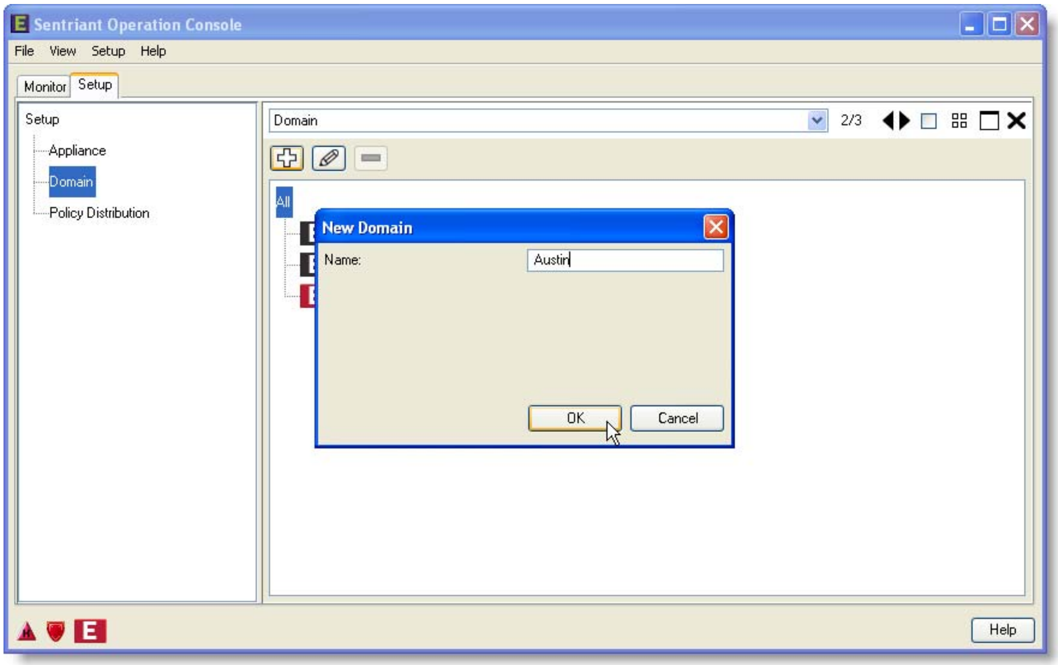
3 The New Domain or Appliance dialog opens. Select **Domain** from the drop-down list.



New Domain or Appliance?

Domain

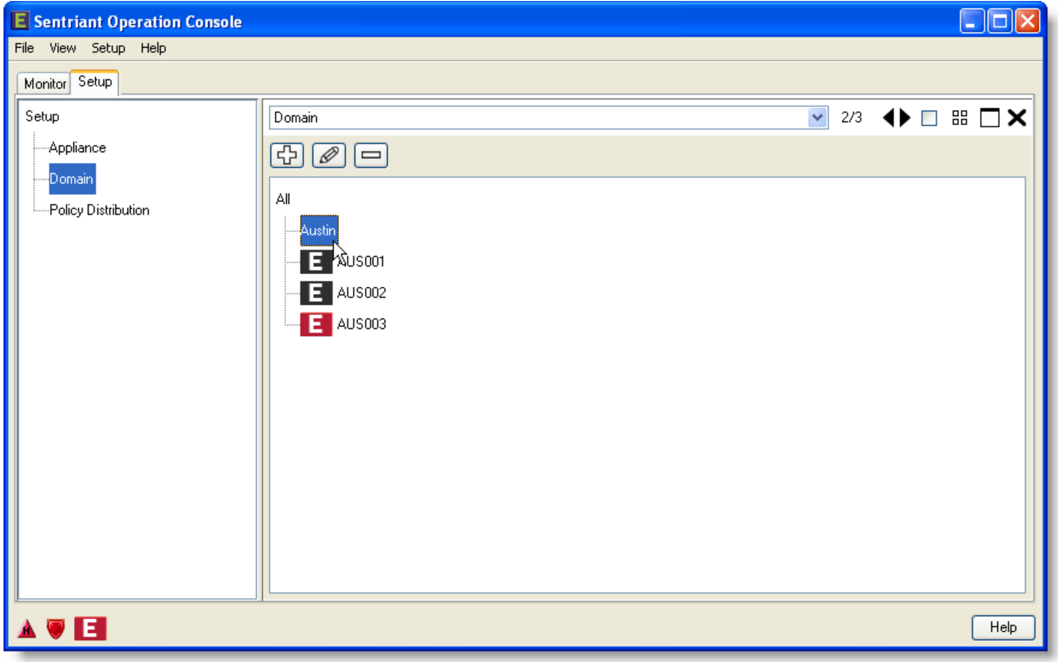
4 Enter a name for the domain and click **OK**.



New Domain

Name: Austin

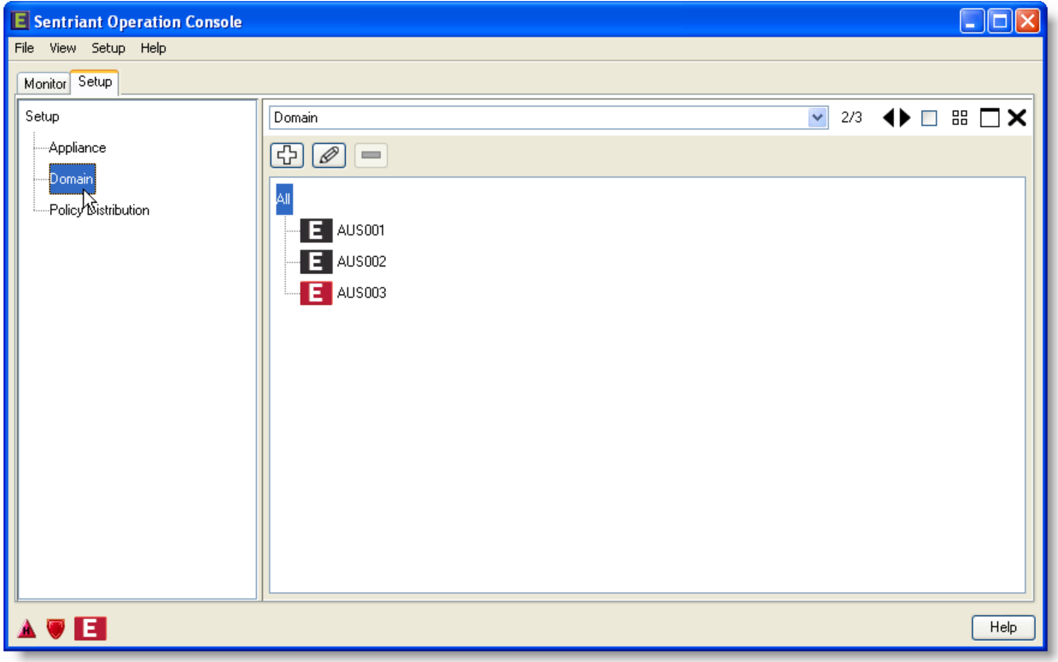
The new domain is added to the information panel.



Viewing Domain Information

To display information about a domain:

1 From the Setup tab, click **Domain**.



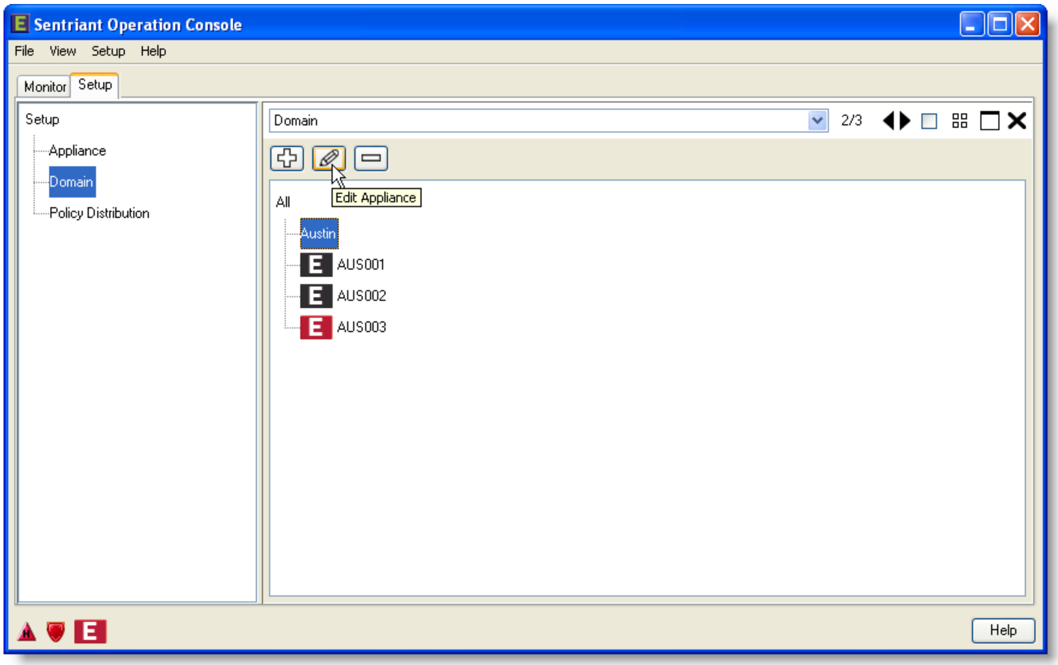
The Domain Panel opens and displays domains and appliances that are members of the SOC. The default domain, All, is shown in the Information Panel along with any appliances that have been added as members.

Deleting Domains

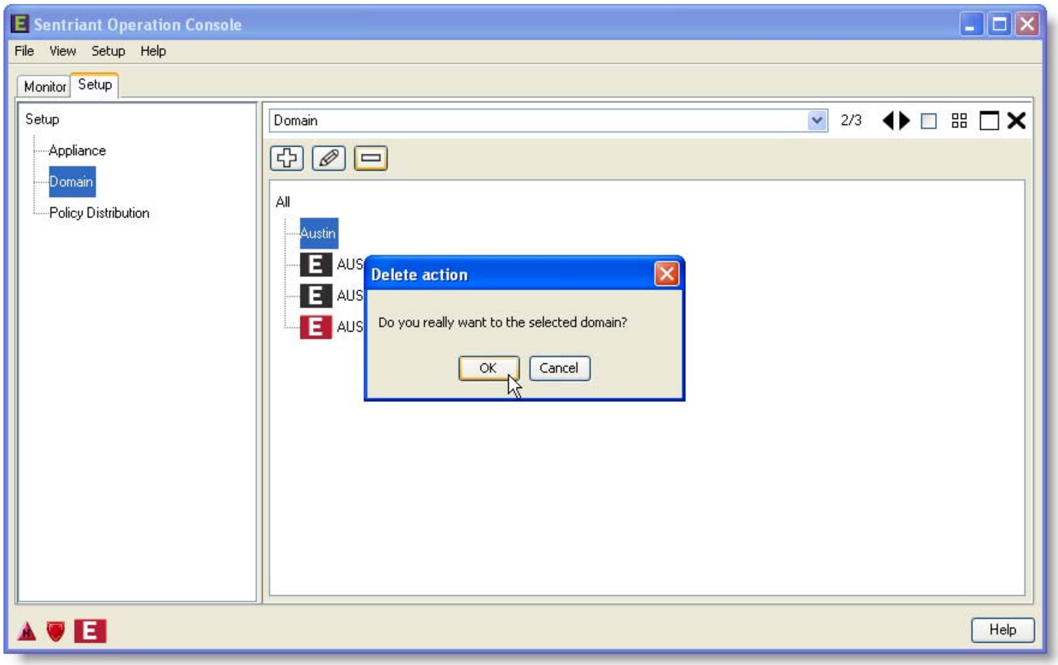
To delete a domain:

1 From the Setup Tab select **Domain**.

2 Click the **Delete Domain/Appliance** button or right-click the domain and select Delete Domain.

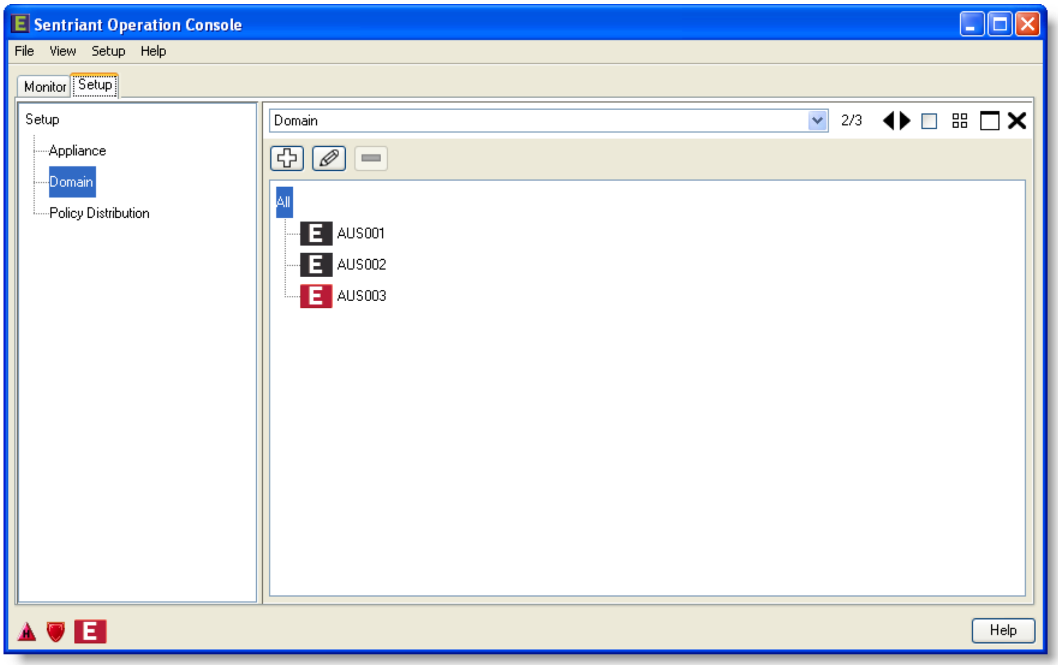


3 The Delete action dialog opens. Click **OK**.



Do you really want to the selected domain?

The domain is deleted from SOC.

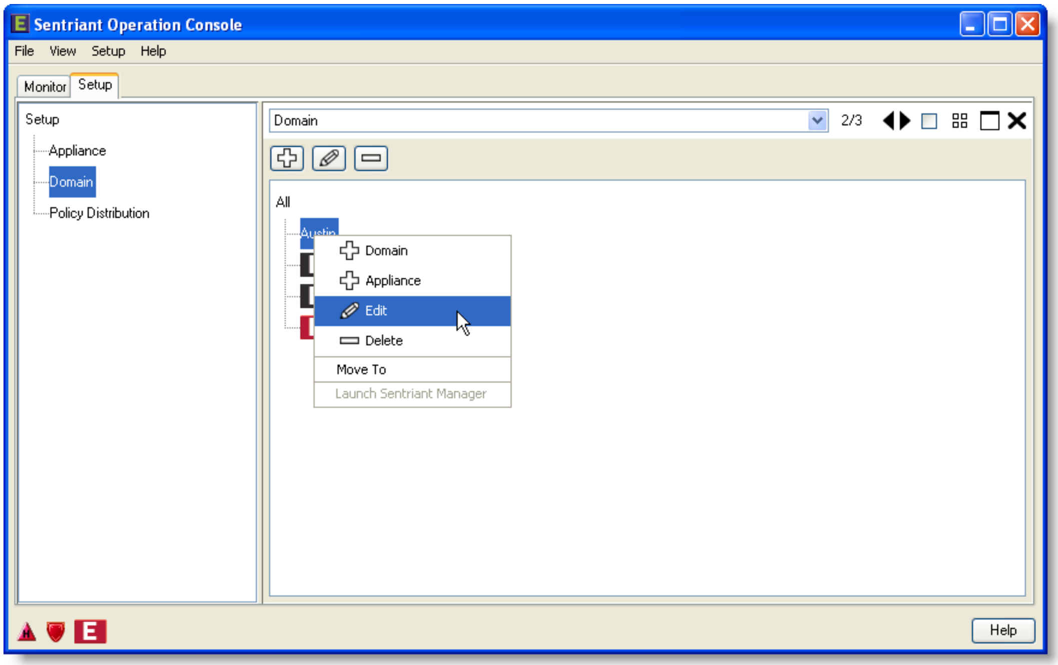


Editing Domains

To edit a domain from SOC:

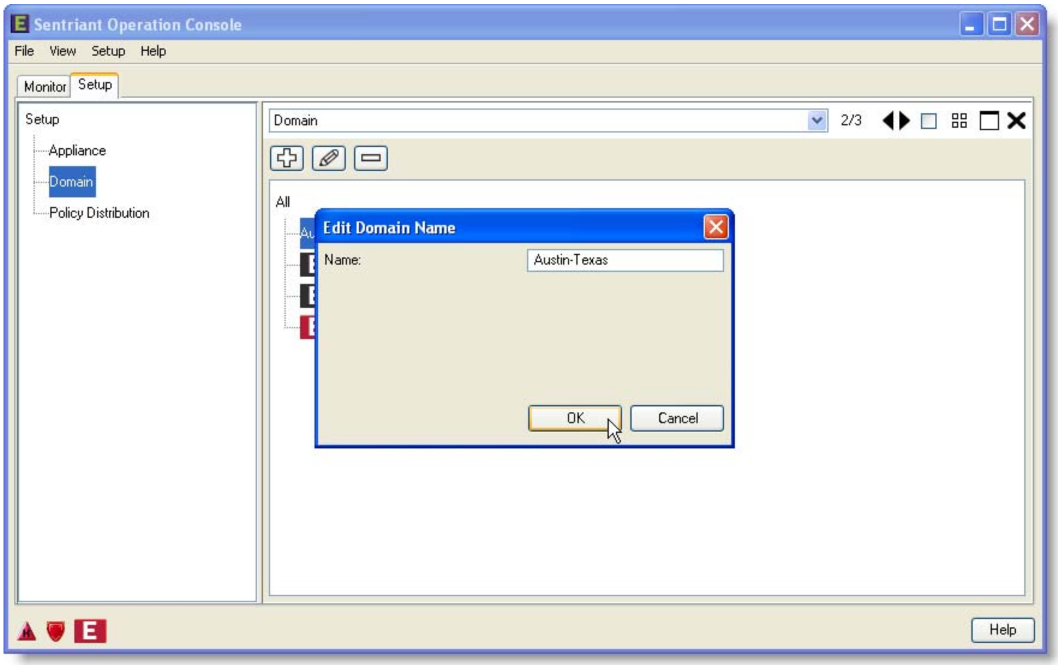
1 From the Setup Tab, select **Domain**.

2 Click the **Edit Domain/Appliance** button or right-click and select Edit.



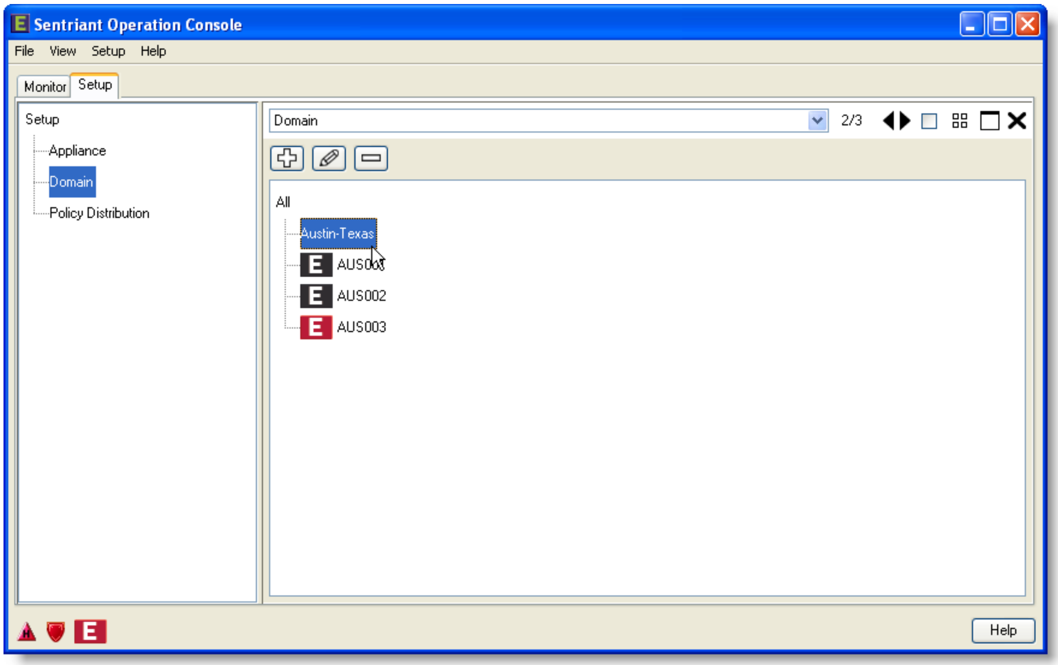
3 The Edit Domain Name dialog opens. Enter a new name for domain.

4 Click **OK**.



Name: Austin-Texas

The domain name has changed and is displayed in the Information Panel.

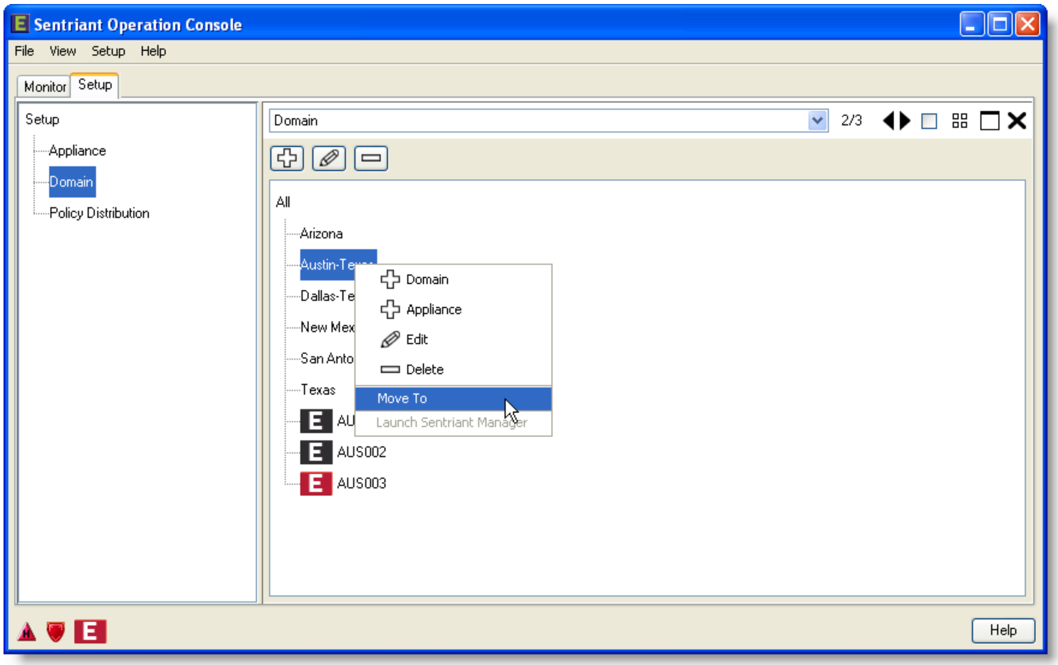


Moving a Domain

To move a domain:

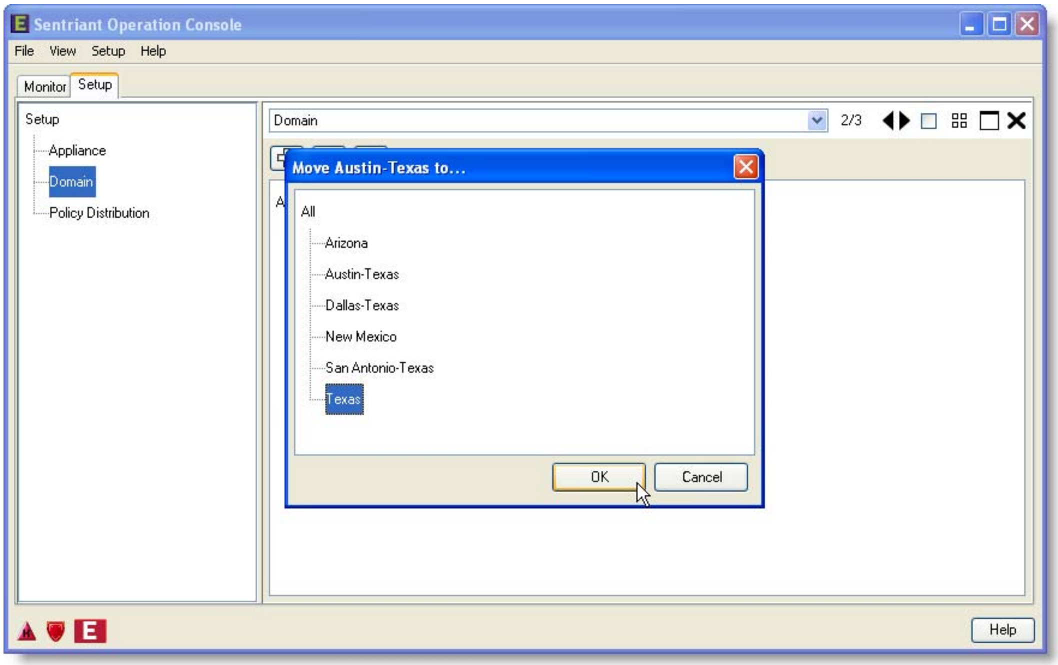
1 From the Setup Tab, select **Domain**.

2 Right-click a domain and select **Move To**.

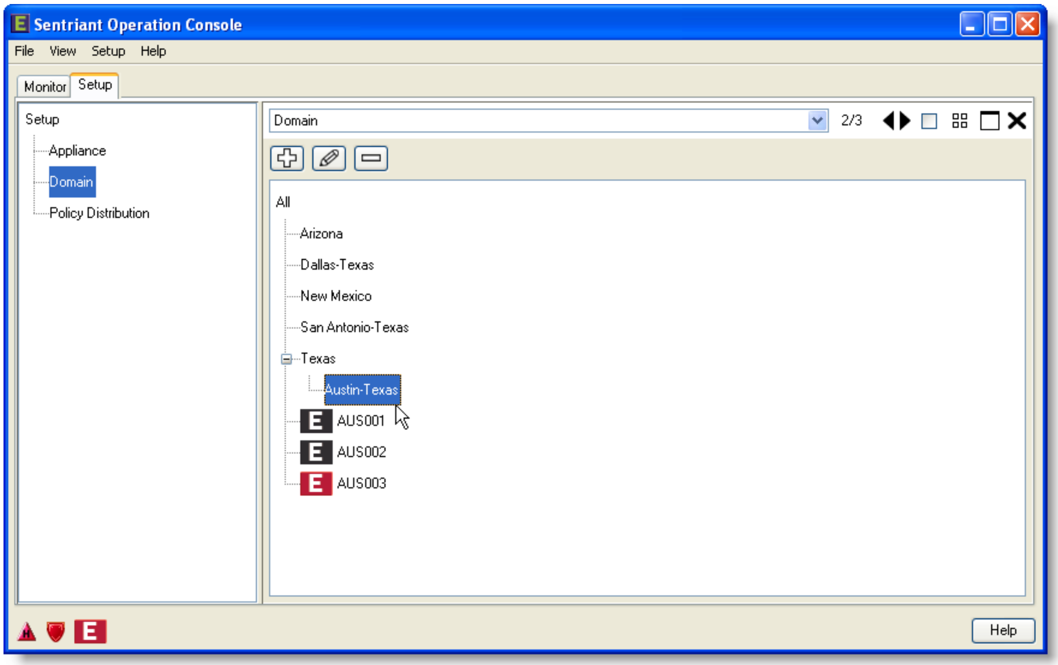


3 The Move To dialog opens. From the list, select a domain. This domain is where the selected domain will be moved under.

4 Click **OK**.



The domain now resides under the selected domain.



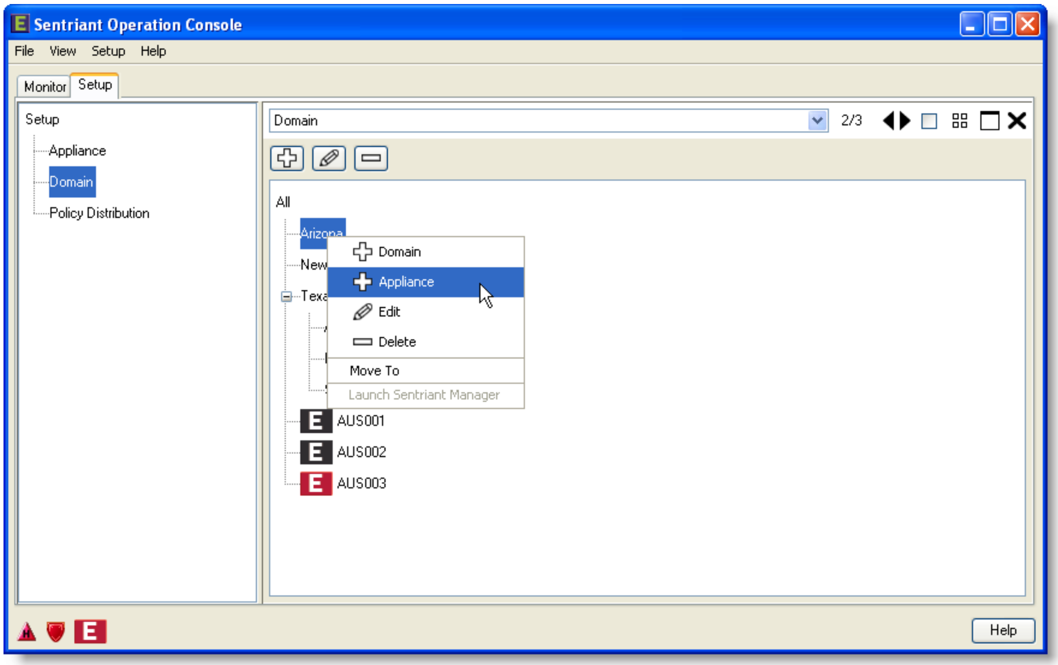
Adding Appliances to SOC from the Domain Panel

Appliances may be added as a member of SOC from the Domain Panel. This is beneficial when creating a new environment with multiple domains. You can create a domain and then begin to add appliances directly to the domain.

To Add an appliance to SOC from the Domain Panel:

1 From the Setup Tab select **Domain**.

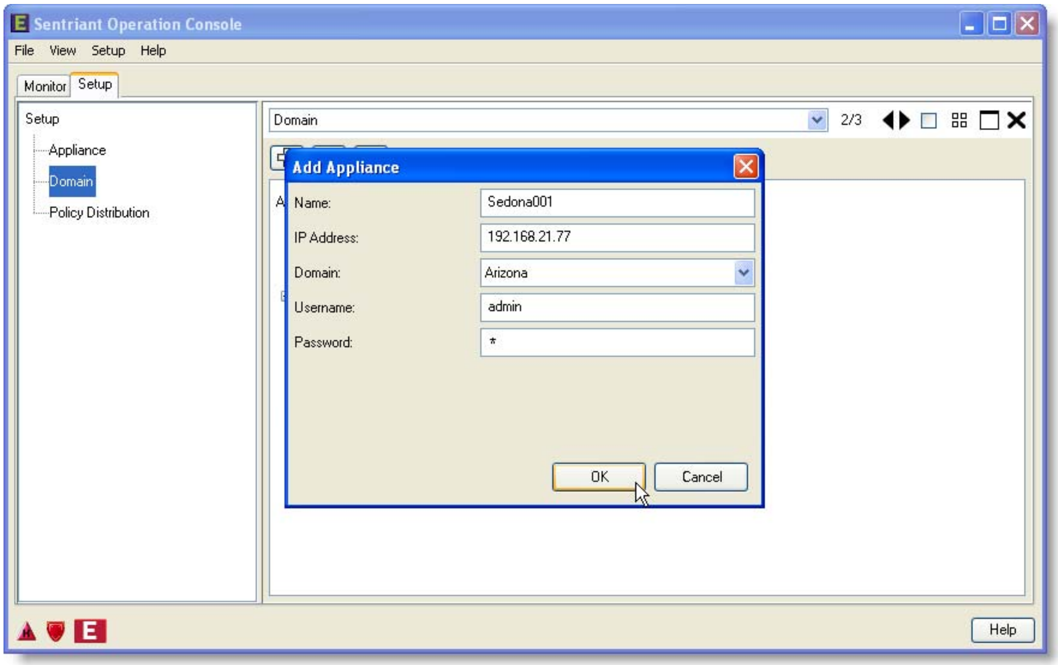
2 Click the **New Domain/Appliance** button or right click on a domain and select **Add Appliance**.



3 Enter the name and IP Address of the appliance. Note: the domain has already been selected.

4 Enter the username and password.

5 Click **OK.**



Name: Sedona001

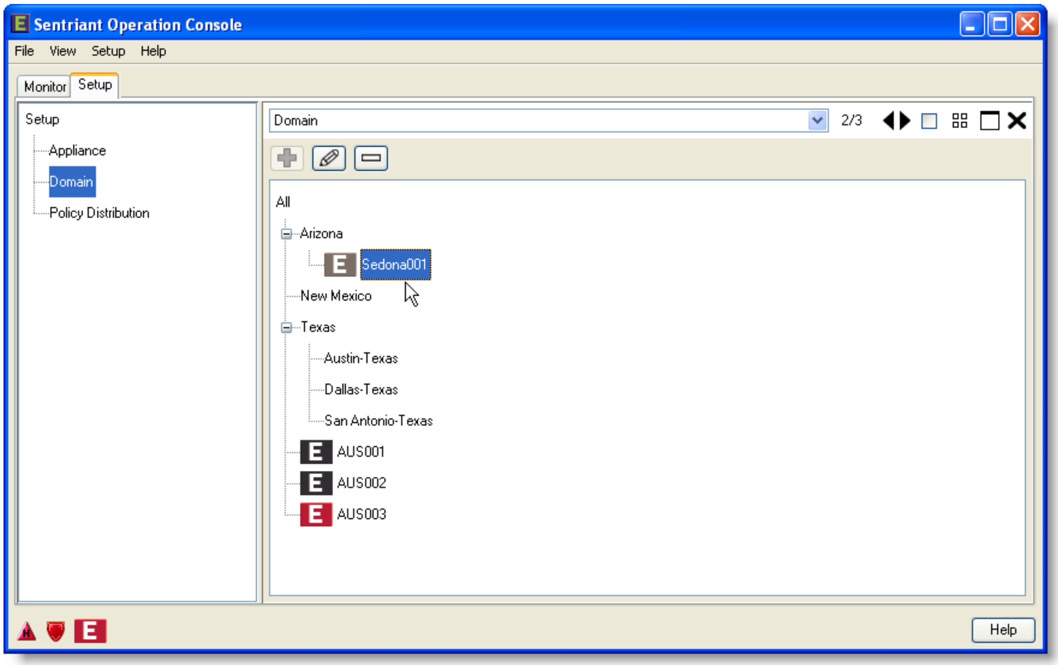
IP Address: 192.168.21.77

Domain: Arizona

Username: admin

Password: *

The appliance is added as a member of SOC and placed under the selected domain.

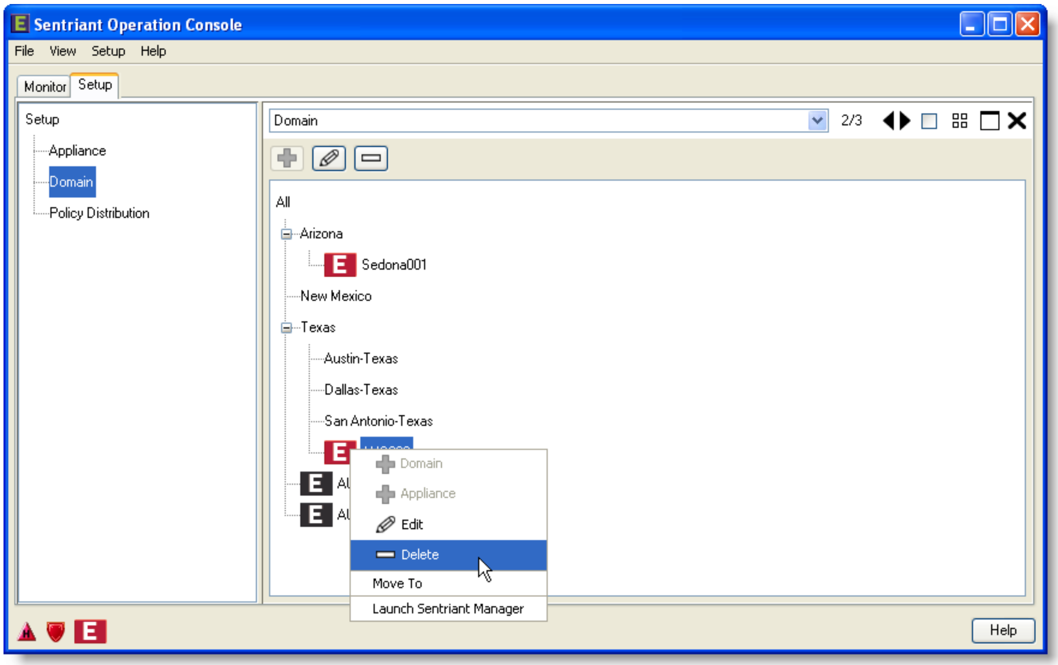


Removing Appliances from the Domain Panel

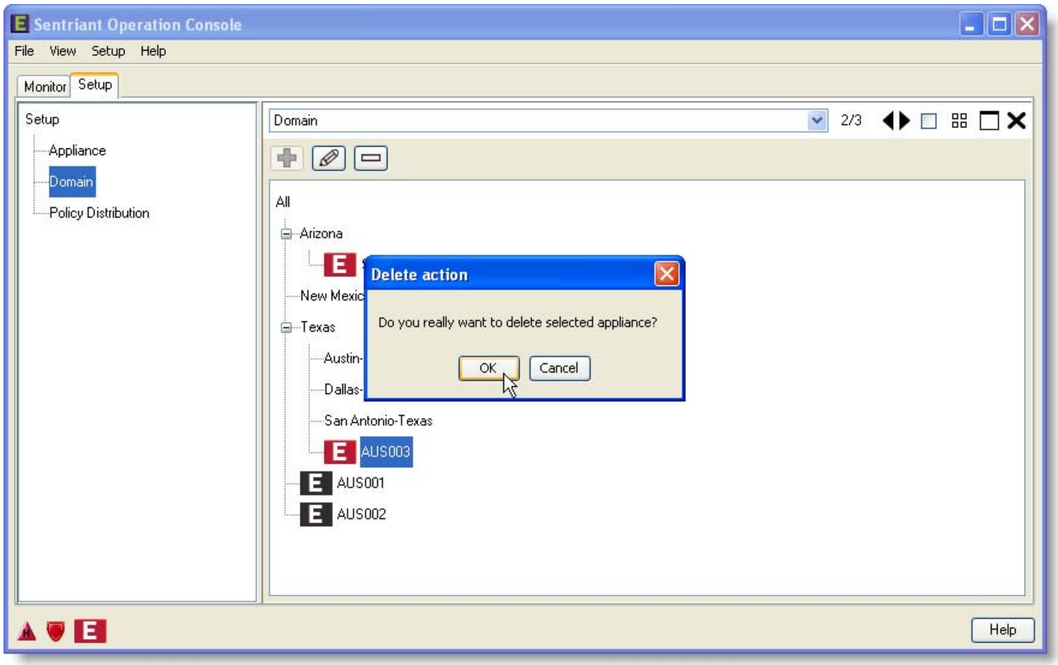
To remove appliances from the Domain Panel:

1 From the Setup Tab, select **Domain**.

2 Click the **Delete Domain/Appliance** button or right-click and select **Remove Appliance**.

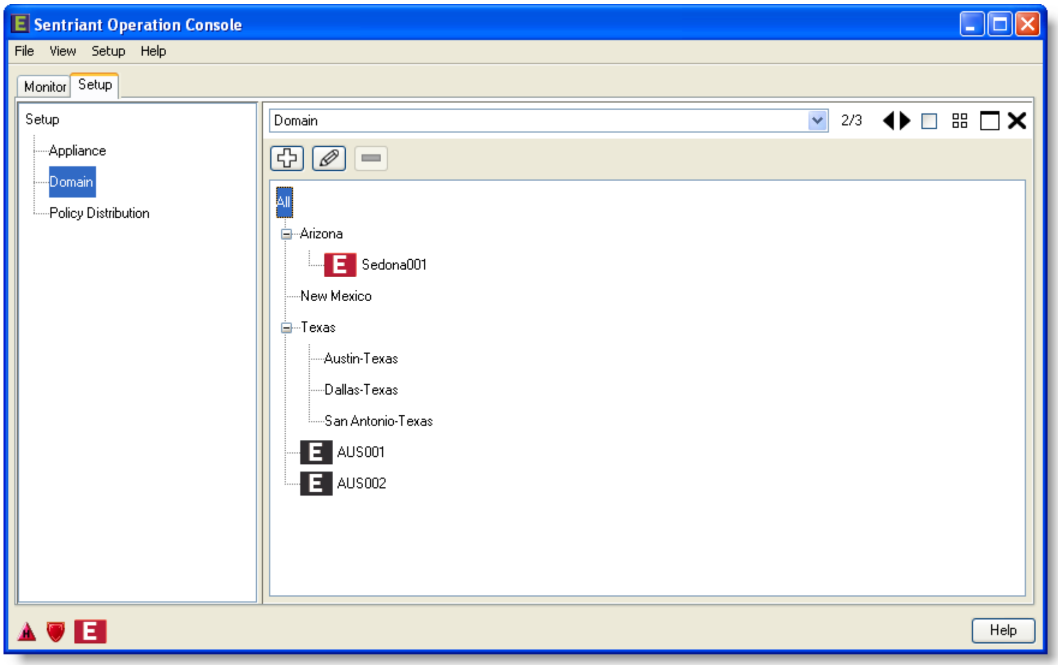


3 The Delete action dialog opens. Click **OK**.



Do you really want to delete selected appliance?

The appliance is removed from SOC.



NOTE

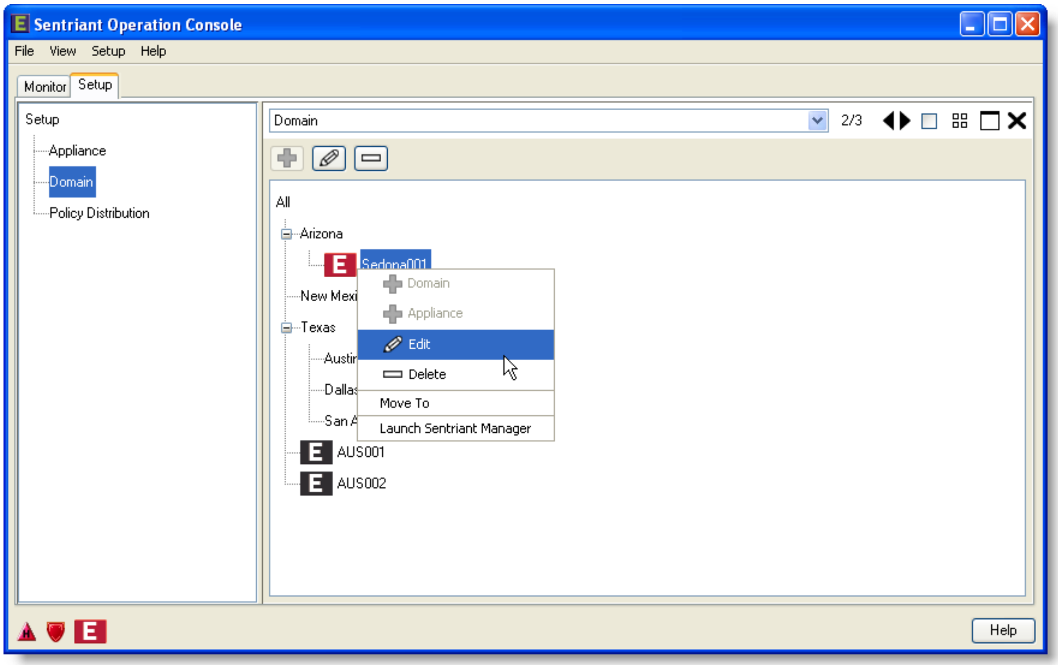
The appliance is still monitoring and mitigating traffic on the network.

Editing Appliances from the Domain Panel

To edit an appliance from the domain panel:

1 From the Setup Tab, select **Domain**.

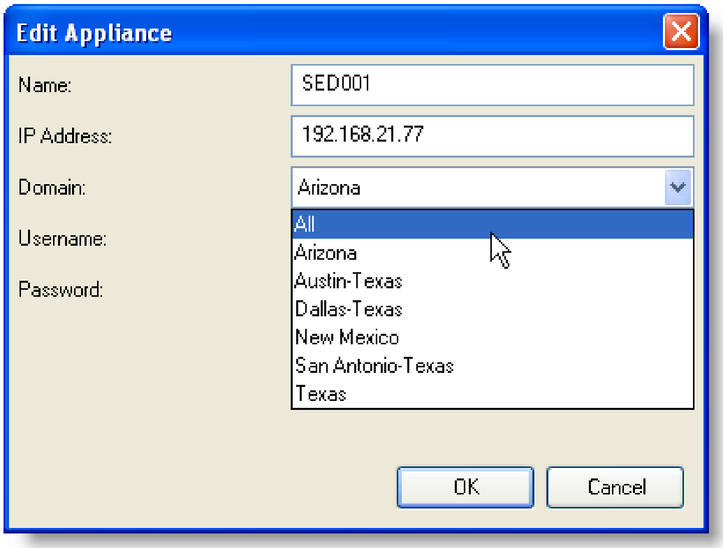
2 Click the **Edit Appliance** button or right-click and select **Edit Appliance**.



The Edit Appliance dialog opens.

3 Edit the Name, IP Address as necessary.

4 If moving the appliance to another domain, select the domain from the drop-down list.



Name: SED001

IP Address: 192.168.21.77

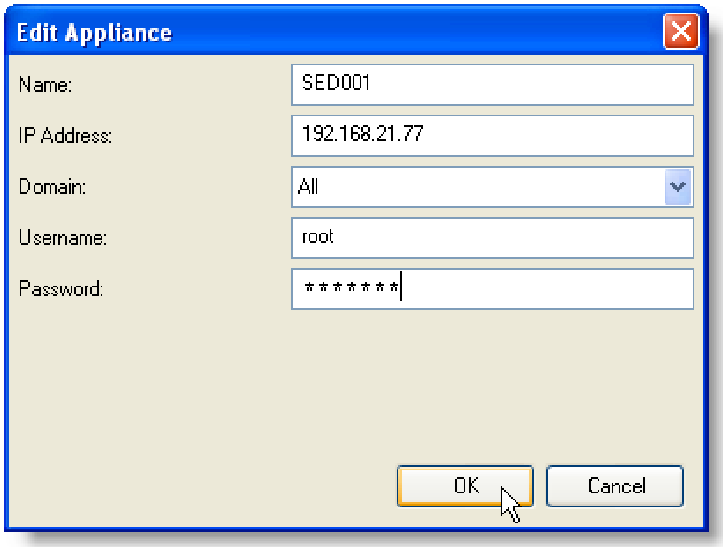
Domain: Arizona

Username:

Password:

5 Edit the Username and password.

6 Click **OK**.



Name: SED001

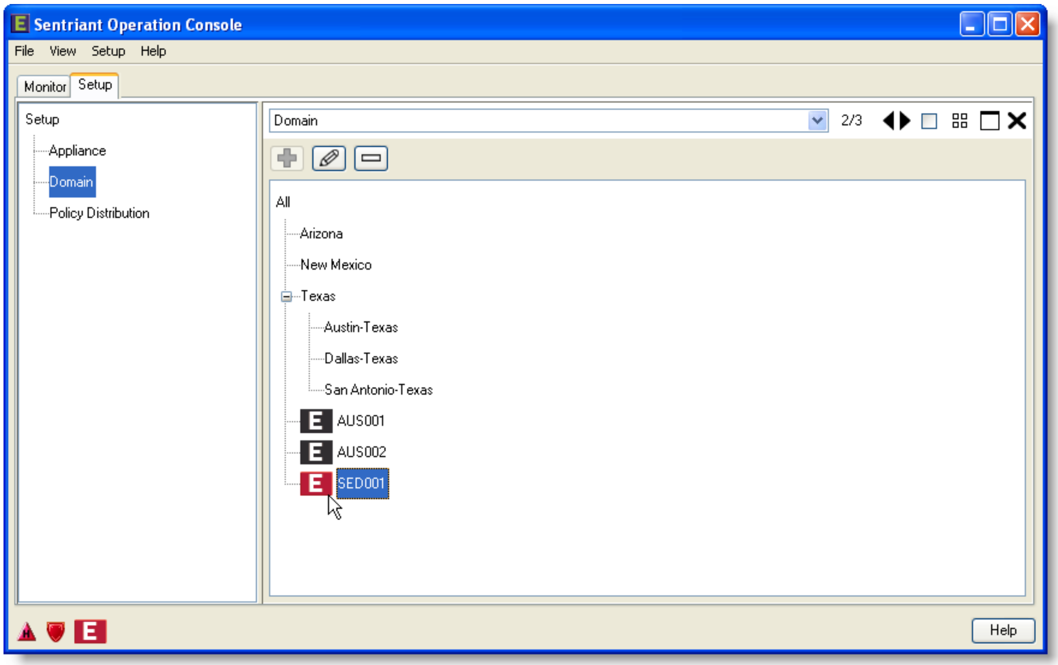
IP Address: 192.168.21.77

Domain: All

Username: root

Password: *******

The appliance is updated with the new parameters.

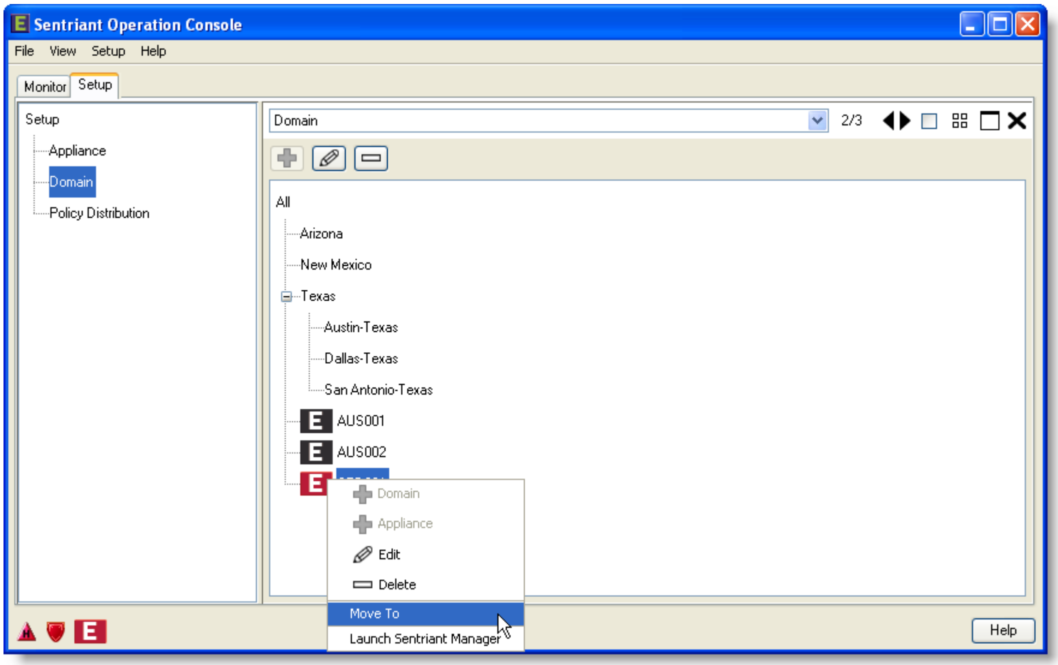


Moving an Appliance

To move an appliance:

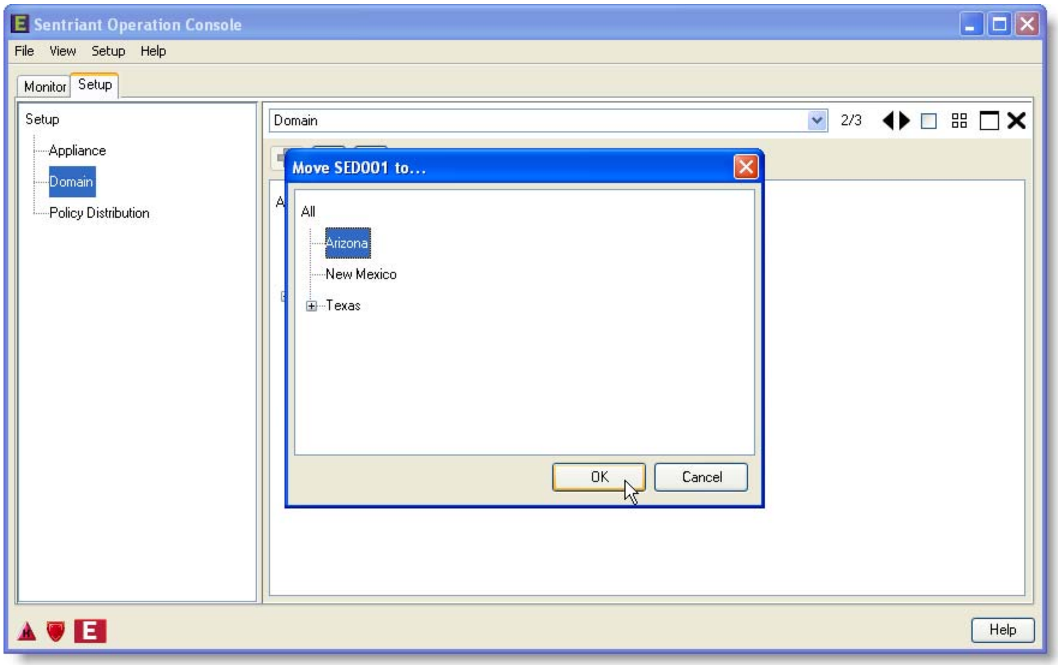
1 From the Setup Tab, select **Domain**.

2 Right-click an appliance and select **Move To**.

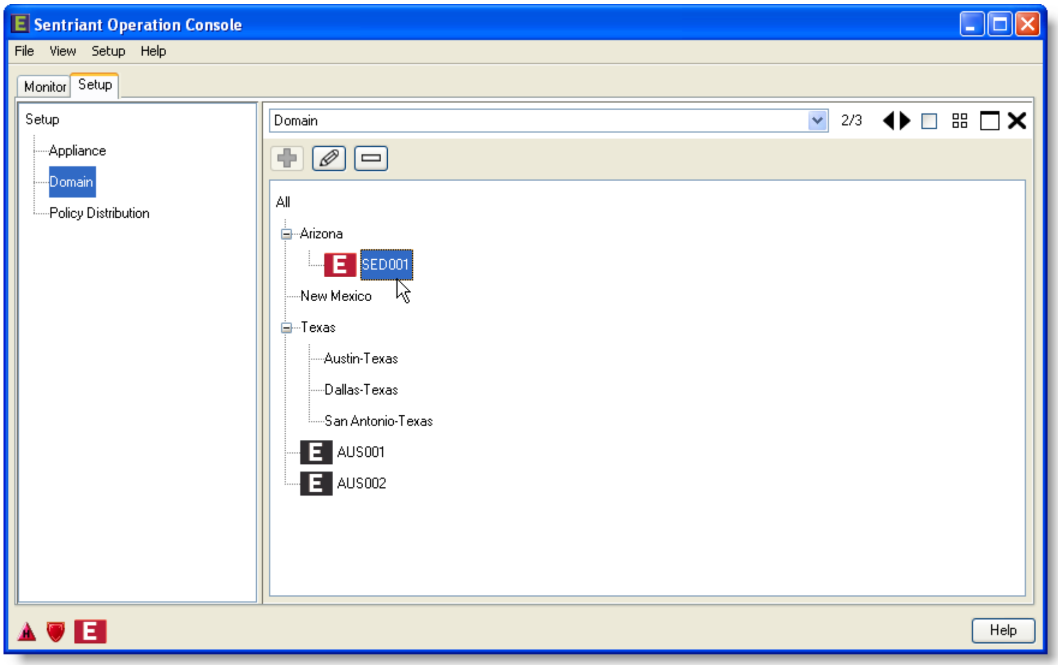


3 The Move To dialog opens. From the list, select a domain. This domain is where the appliance will be moved under.

4 Click **OK**.



The appliance now resides under the selected domain.

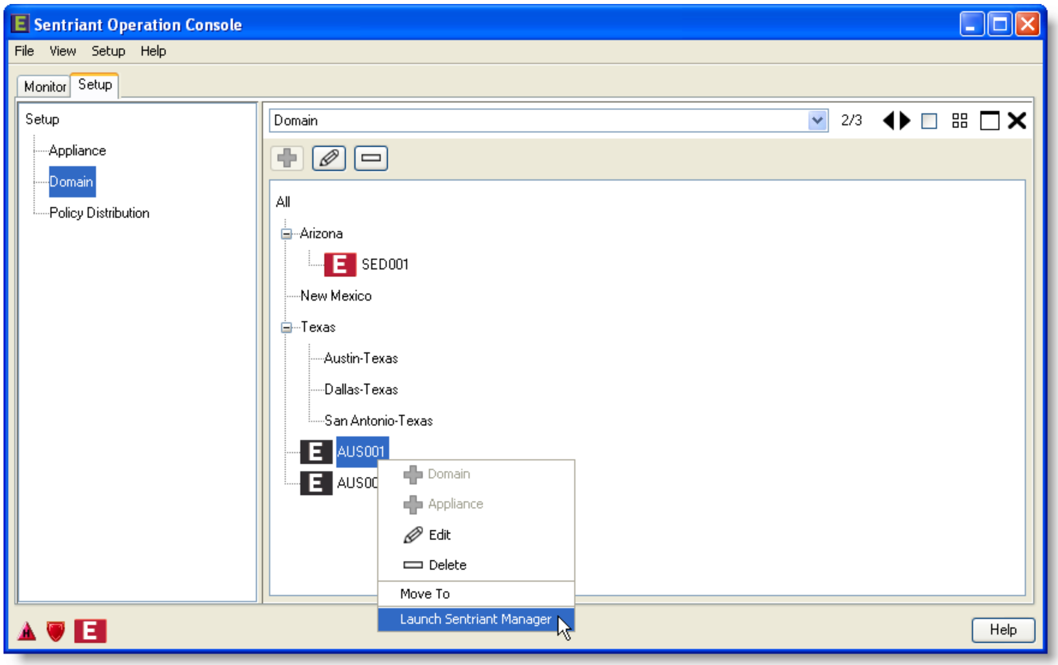


Launch Sentriant Manager from the Domain Panel

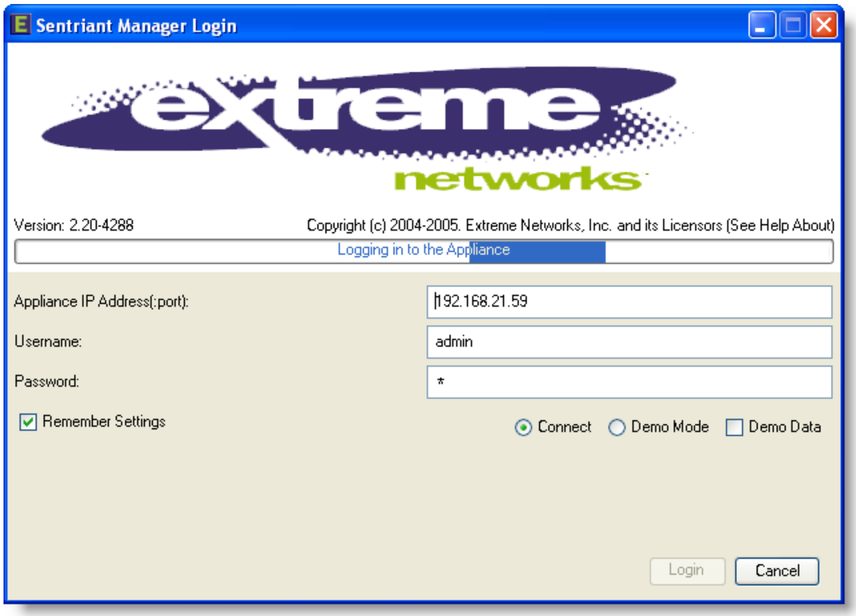
To launch Sentriant Manager from the Domain Panel:

1 From the Setup Tab, select **Domain**.

2 Right-click an appliance and select **Launch Sentriant Manager**.



The Sentriant Manager Login dialog opens and begins the login process. Note that the appliance parameters have already been populated.



Sentriant Manager Login

Version: 2.20-4288

Copyright (c) 2004-2005. Extreme Networks, Inc. and its Licensors (See Help About)

Logging in to the Appliance

Appliance IP Address(:port): 192.168.21.59

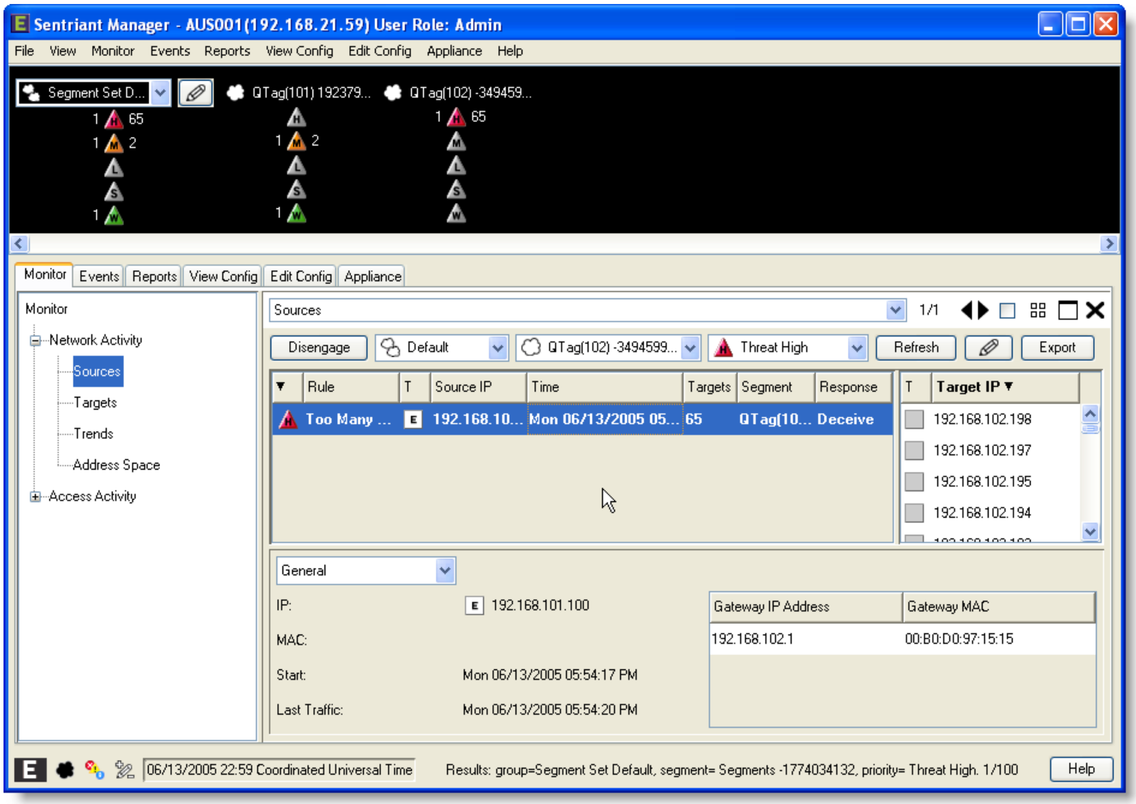
Username: admin

Password: *

☑ Remember Settings

● Connect ○ Demo Mode □ Demo Data

Once the Sentriant Manager is up and running, focus is placed on the panel where you launched Sentriant Manager. In this case, Sentriant Manager was launched from Setup > Domain. Therefore, Sentriant Manager will open and navigate to the Monitor Panel.



Sentriant Manager - AUS001(192.168.21.59) User Role: Admin

▼	Rule	T	Source IP	Time	Targets	Segment	Response
H	Too Many ...	E	192.168.10...	Mon 06/13/2005 05...	65	QTag(10...	Deceive

T	Target IP ▼
□	192.168.102.198
□	192.168.102.197
□	192.168.102.195
□	192.168.102.194

IP: E 192.168.101.100

MAC:

Start: Mon 06/13/2005 05:54:17 PM

Last Traffic: Mon 06/13/2005 05:54:20 PM

Gateway IP Address	Gateway MAC
192.168.102.1	00:B0:D0:97:15:15

06/13/2005 22:59 Coordinated Universal Time

Results: group=Segment Set Default, segment= Segments -1774034132, priority= Threat High. 1/100

Policy Distribution Panel

The Policy Panel is where you will create, distribute and maintain policy distributions.

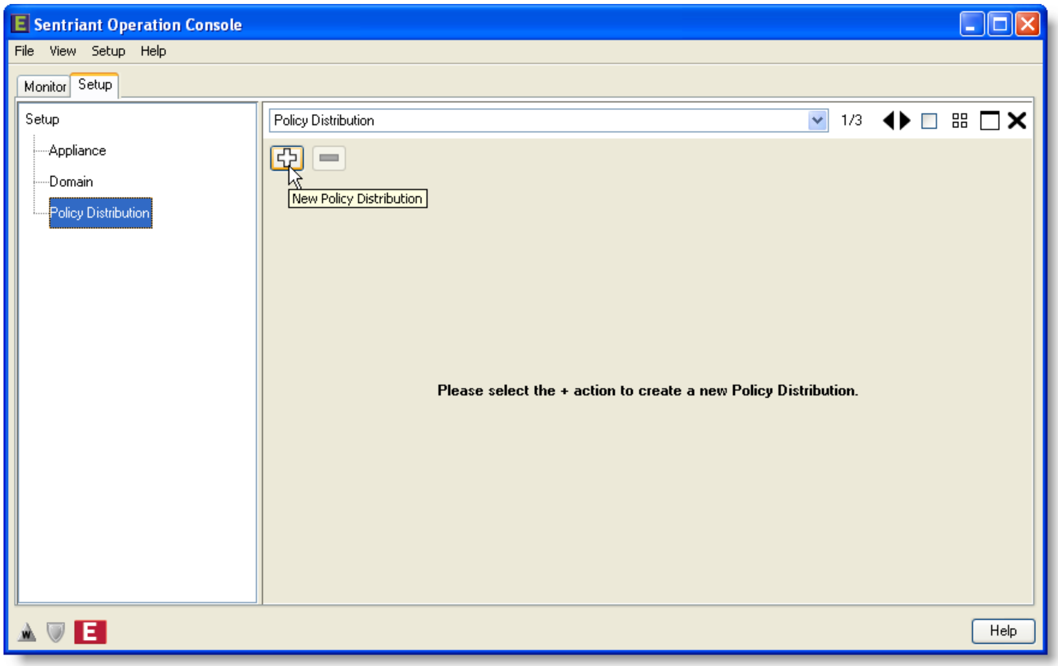
The Policy Panel consists of an Information Panel where you create policy distributions and apply them to appliances. A policy distribution is a set of threat rules configured on a Sentriant appliance that have detection and mitigation settings based on the type of deployment. SOC has the ability to capture the policy from one Sentriant appliance and send it to other appliances that are members of SOC.

Creating a Policy Distribution

Adding a policy distribution:

1 From the Setup Tab select **Policy Distribution**.

2 Click the **New Policy Distribution** button.



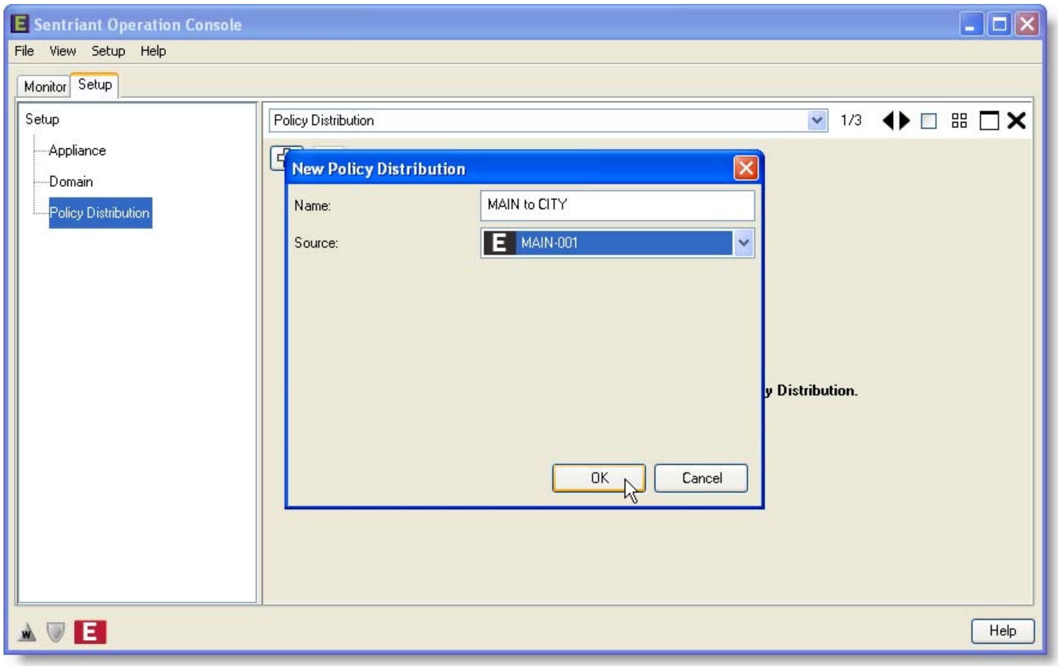
Please select the + action to create a new Policy Distribution.

3 Enter a name and select a source appliance from the drop-down list. The policy configuration on the source appliance will be sent to appliances in the distribution list.

NOTE

The appliances in the distribution list must be the same version as the source appliance.

4 Click **OK** to save the policy distribution and close the dialog.



New Policy Distribution

Name: MAIN to CITY

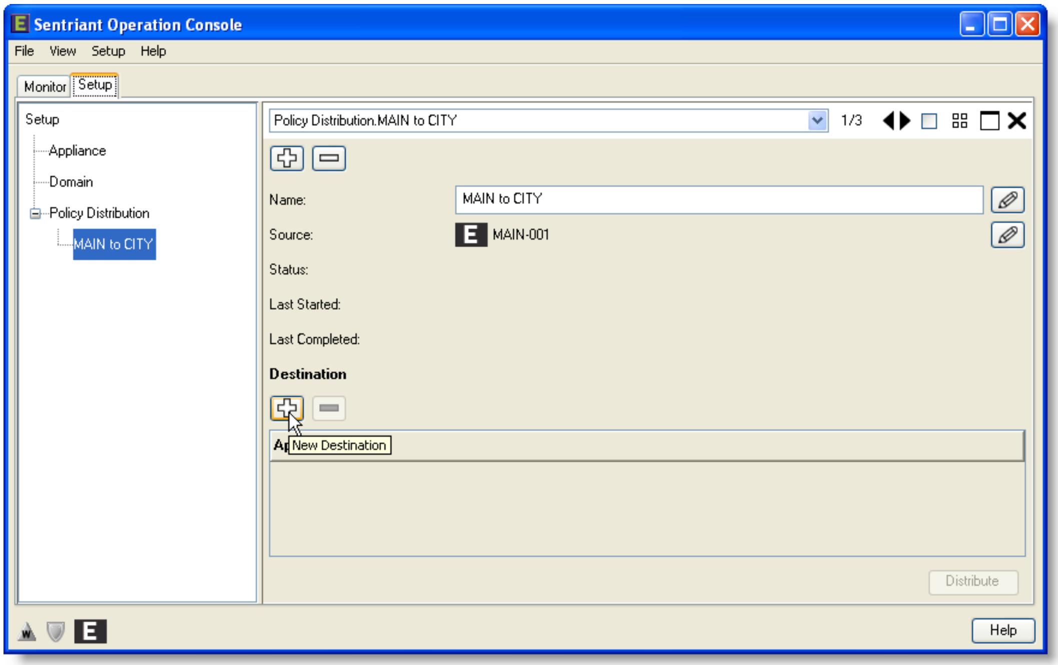
Source: MAIN-001

OK Cancel

Adding Destinations.

Once the source appliance has been identified, select the appliance which will receive the policy.

5 Click the **New Destination** button.



Policy Distribution.MAIN to CITY

Name: MAIN to CITY

Source: MAIN-001

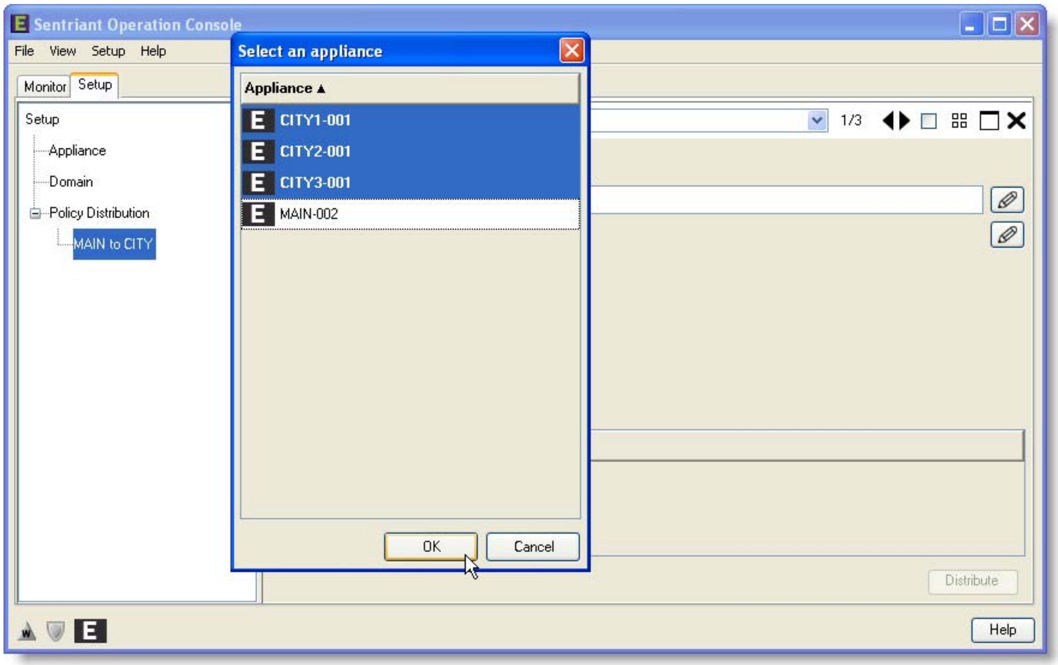
Status:

Last Started:

Last Completed:

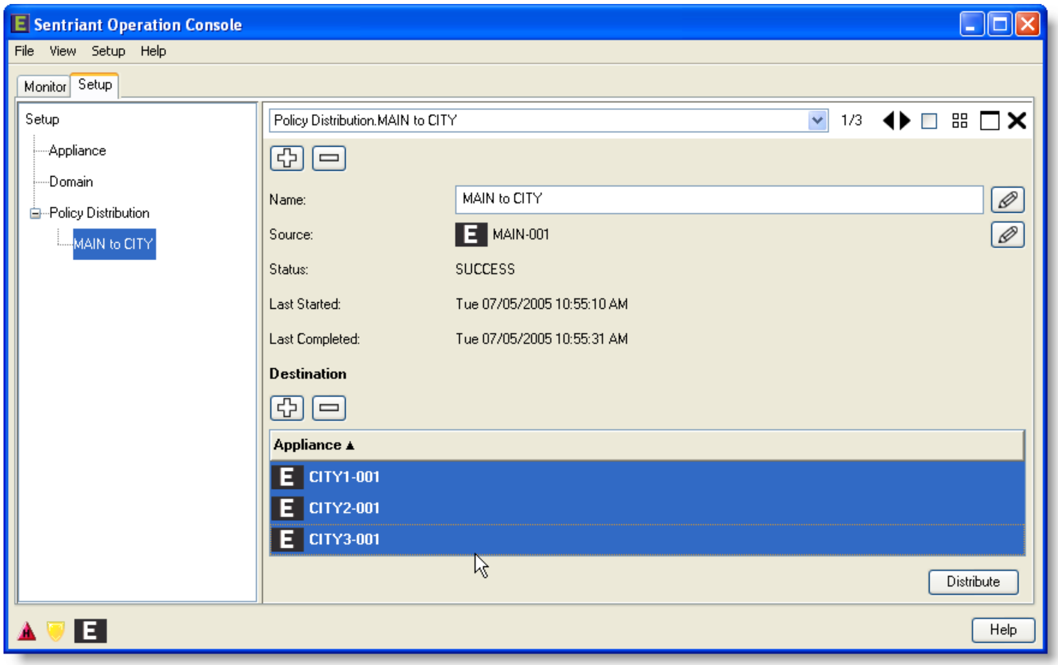
6 Select the appliances that will receive the distribution. You may multi-select appliances from the list.

7 Click **OK**.



Appliance ▲
CITY1-001
CITY2-001
CITY3-001
MAIN-002

The appliances are added to the distribution list. See Starting a Policy Distribution to learn about sending policy distributions to destination appliances.



Name: MAIN to CITY

Source: MAIN-001

Status: SUCCESS

Last Started: Tue 07/05/2005 10:55:10 AM

Last Completed: Tue 07/05/2005 10:55:31 AM

Destination

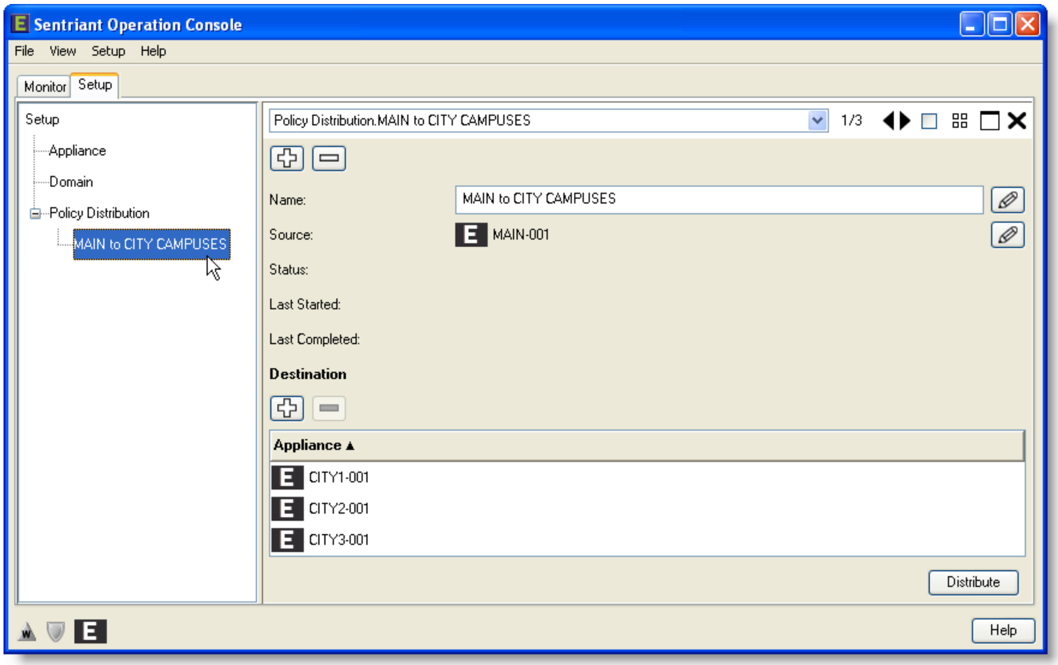
Appliance ▲
CITY1-001
CITY2-001
CITY3-001

Viewing Policy Distribution Information

To view Policy Distributions:

1 From the Setup tab, click **Policy Distribution**.

2 Click a Policy Distribution from the left navigation.



Setup
- Appliance
- Domain
- Policy Distribution
  - MAIN to CITY CAMPUSES

Policy Distribution.MAIN to CITY CAMPUSES 1/3

Name: MAIN to CITY CAMPUSES

Source: MAIN-001

Status:

Last Started:

Last Completed:

Destination

Appliance ▲
CITY1-001
CITY2-001
CITY3-001

The selected Policy Distribution is displayed in the Information Panel with the following:

- Name - policy distribution name
- Source - the appliance selected as the policy source. The source is where the policy will be extracted and sent to appliances in the distribution list.
- Status - the status of a policy distribution
- Last Started - a timestamp when the policy distribution was started
- Last Completed - a timestamp when the policy distribution completed

At the bottom of the screen is where appliances are added to the destination list by clicking the New Destination button and adding appliances from the dialog. Clicking the Distribute button located on the lower right of the screen opens a dialog where you start the distribution.

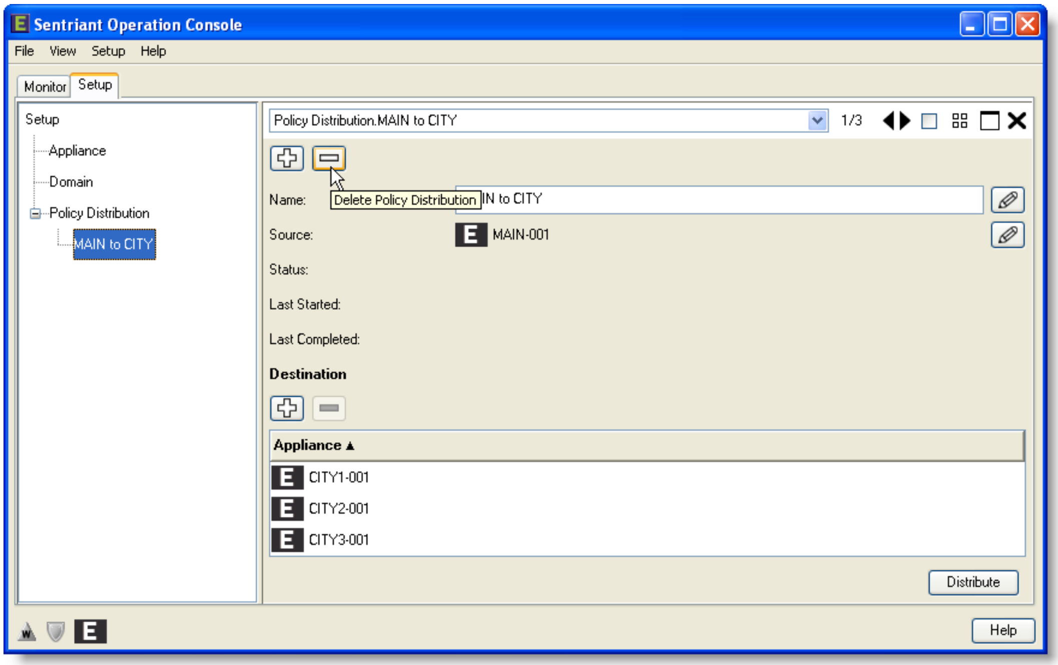
Delete Policy Distribution

To delete a policy distribution:

1 From the Setup Tab select **Policy Distribution**.

2 Select a policy distribution from the left navigation panel.

3 Click the **Delete Policy Distribution** button.



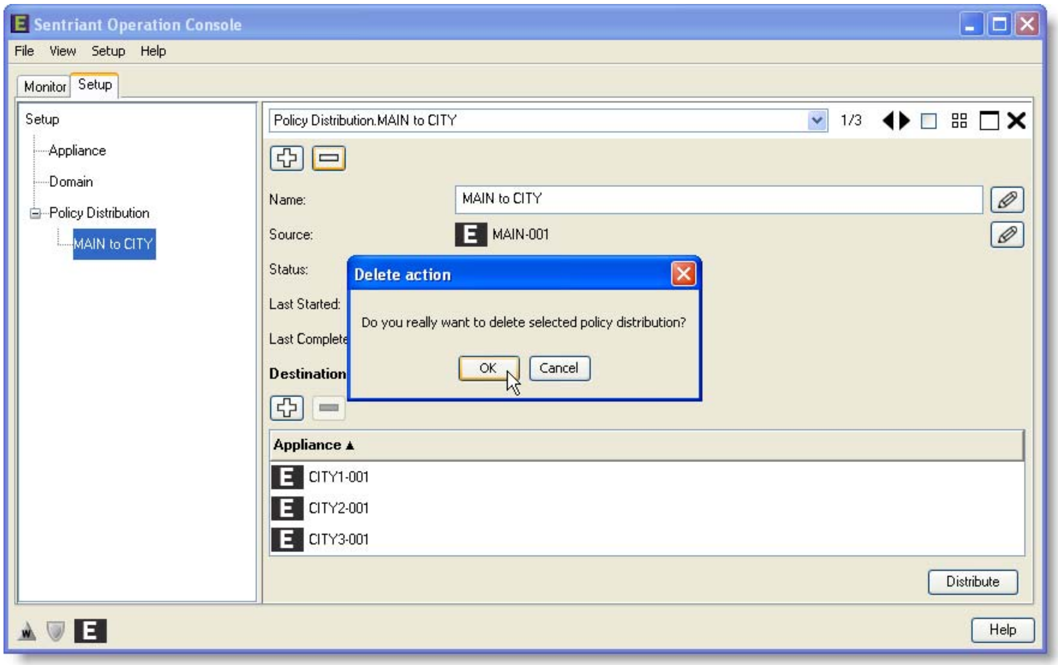
Policy Distribution.MAIN to CITY

Name: IN to CITY

Source: MAIN-001

Appliance ▲
CITY1-001
CITY2-001
CITY3-001

4 The Delete action dialog opens. Click **OK**.



Policy Distribution.MAIN to CITY

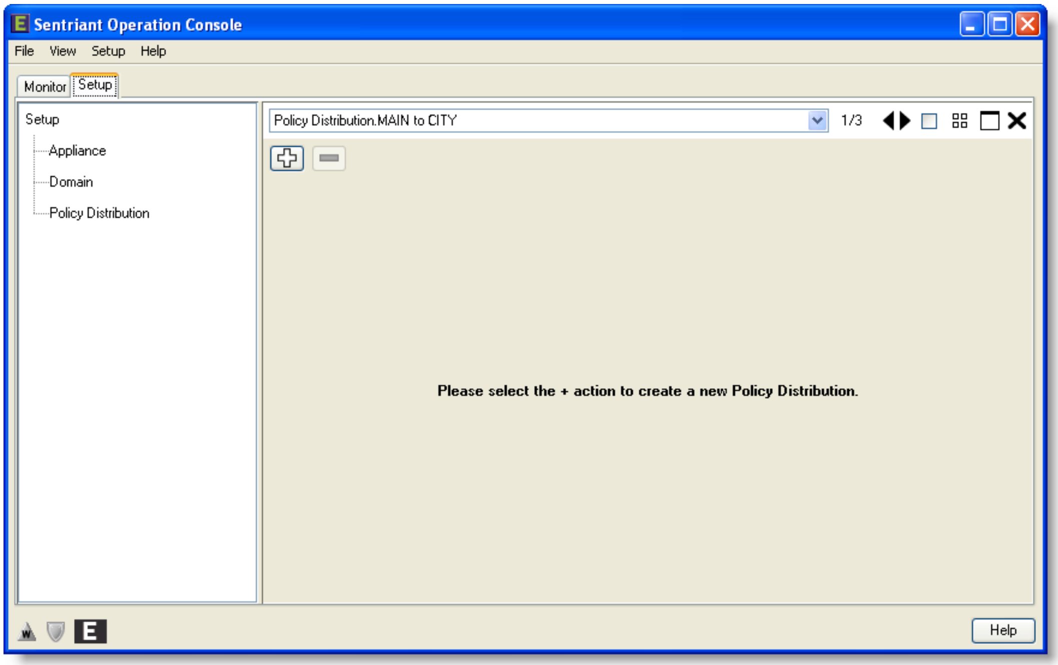
Name: MAIN to CITY

Source: MAIN-001

Do you really want to delete selected policy distribution?

Appliance ▲
CITY1-001
CITY2-001
CITY3-001

The policy distribution is deleted from SOC.



Please select the + action to create a new Policy Distribution.

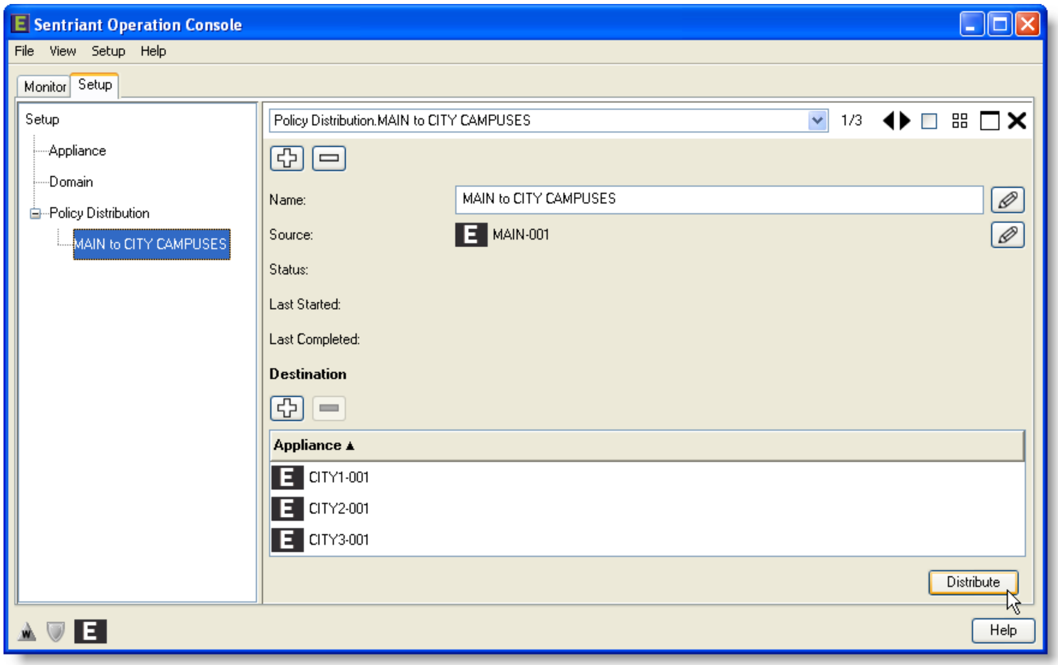
Sending Policy Distributions

To send Policy Distributions:

1 From the Setup Tab select **Policy Distribution**.

2 Select a **Policy Distribution** from the left navigation.

3 Click the **Distribute** button at the lower right of the panel.



Name: MAIN to CITY CAMPUSES

Source: MAIN-001

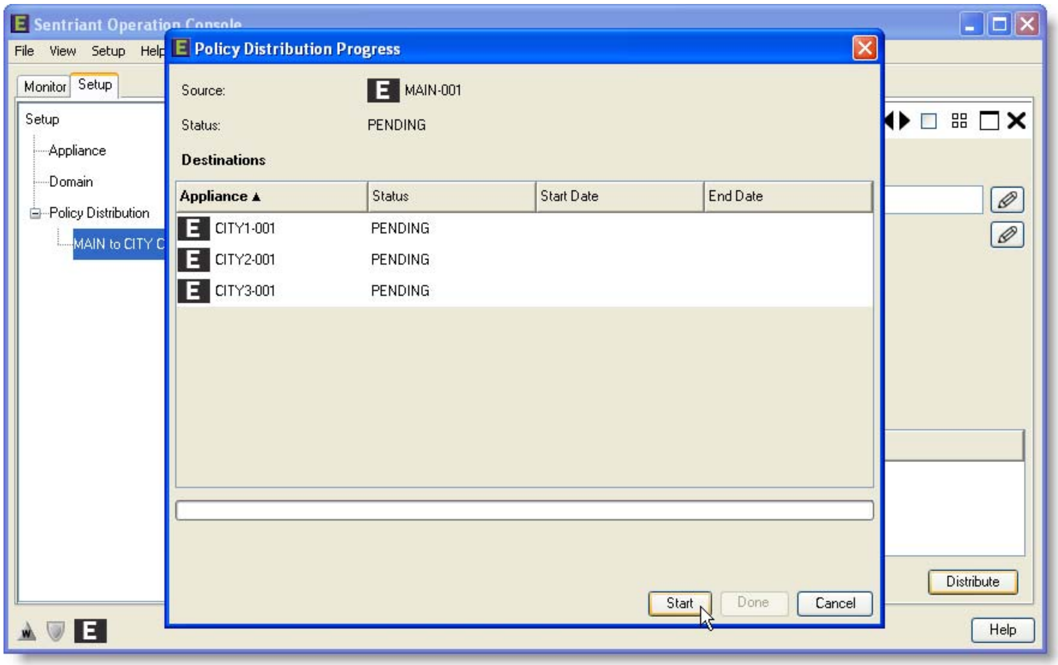
Status:

Last Started:

Last Completed:

Appliance ▲
CITY1-001
CITY2-001
CITY3-001

The Policy Distribution Progress dialog opens with the list and status of appliances which will receive the policy. Click **Start** to begin the distribution.



Source: MAIN-001

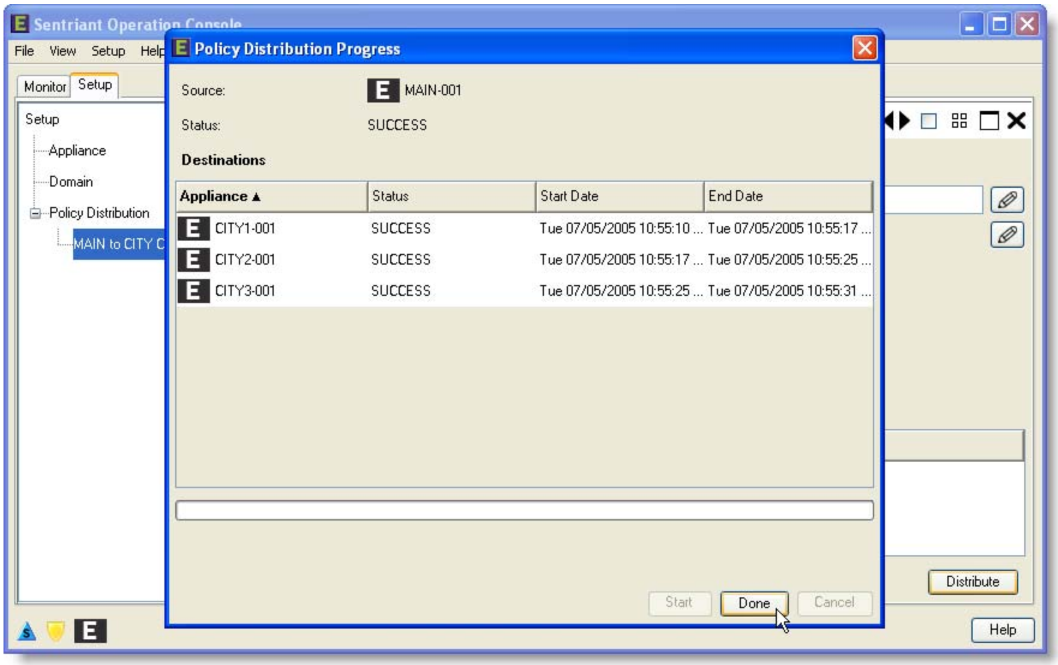
Status: PENDING

Destinations

Appliance ▲	Status	Start Date	End Date
CITY1-001	PENDING		
CITY2-001	PENDING		
CITY3-001	PENDING		

As the distribution progresses, the status for each appliance will be updated. Once the distribution has completed, the status is updated to Success and the start end timestamps are updated.

4 Click **Done** to close the dialog.



Source: MAIN-001

Status: SUCCESS

Destinations

Appliance ▲	Status	Start Date	End Date
CITY1-001	SUCCESS	Tue 07/05/2005 10:55:10 ...	Tue 07/05/2005 10:55:17 ...
CITY2-001	SUCCESS	Tue 07/05/2005 10:55:17 ...	Tue 07/05/2005 10:55:25 ...
CITY3-001	SUCCESS	Tue 07/05/2005 10:55:25 ...	Tue 07/05/2005 10:55:31 ...

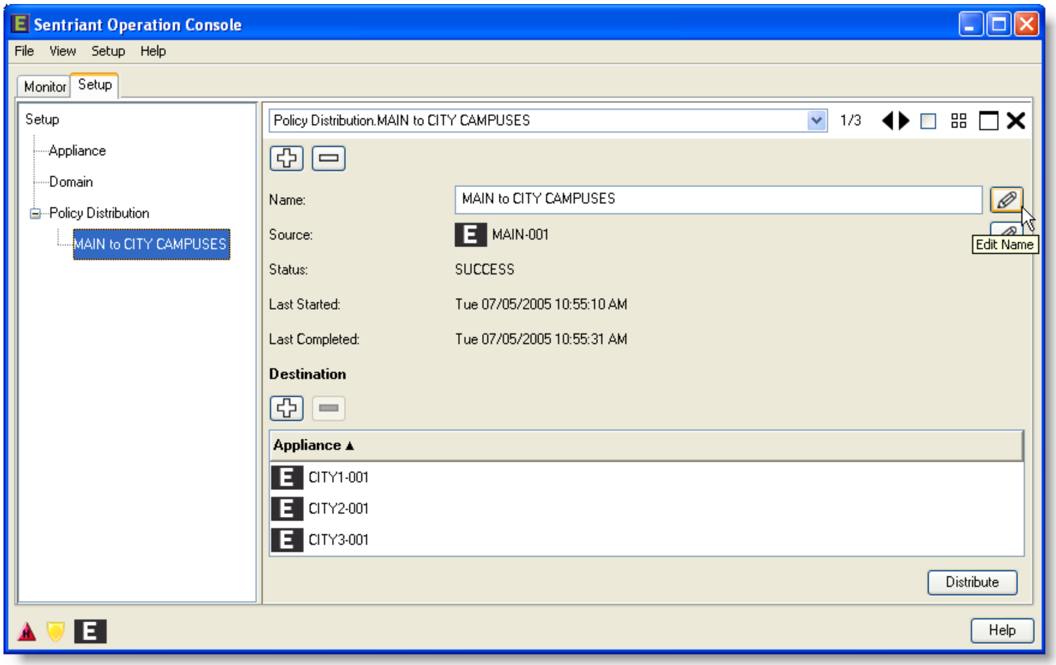
Editing Policy Distribution

To edit the name of a policy distribution:

1 From the Setup Tab, select **Policy Distribution**.

2 Select a policy distribution from the left navigation panel.

3 Click the **Edit Name** button.



Policy Distribution.MAIN to CITY CAMPUSES

Name: MAIN to CITY CAMPUSES

Source: MAIN-001

Status: SUCCESS

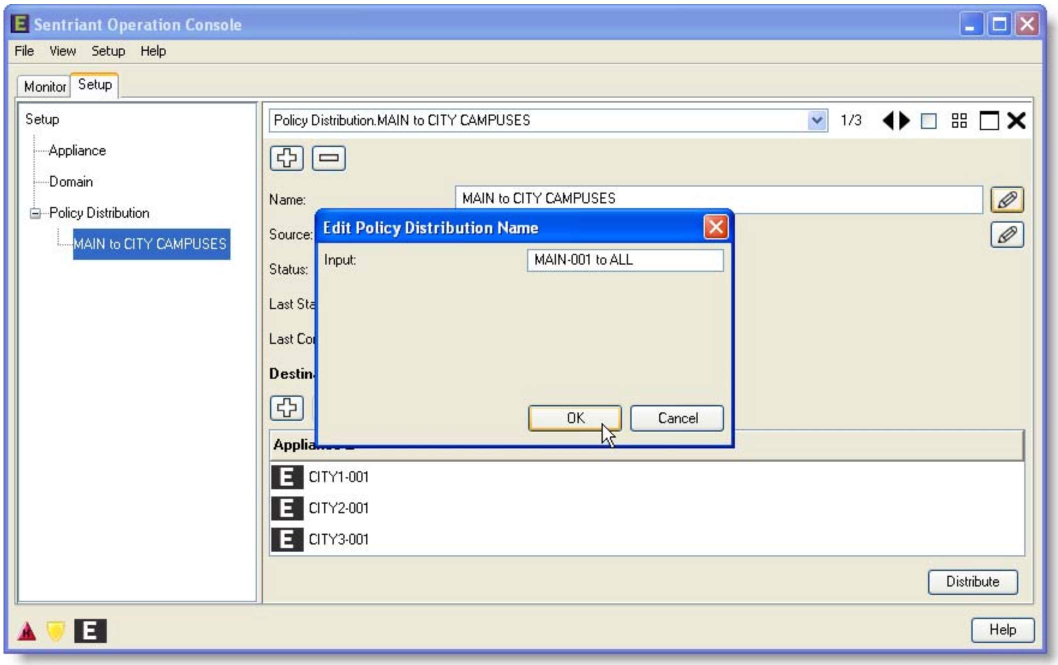
Last Started: Tue 07/05/2005 10:55:10 AM

Last Completed: Tue 07/05/2005 10:55:31 AM

Appliance ▲
CITY1-001
CITY2-001
CITY3-001

4 The Edit Policy Distribution Name dialog opens. Enter a new name.

5 Click **OK**.



Policy Distribution.MAIN to CITY CAMPUSES

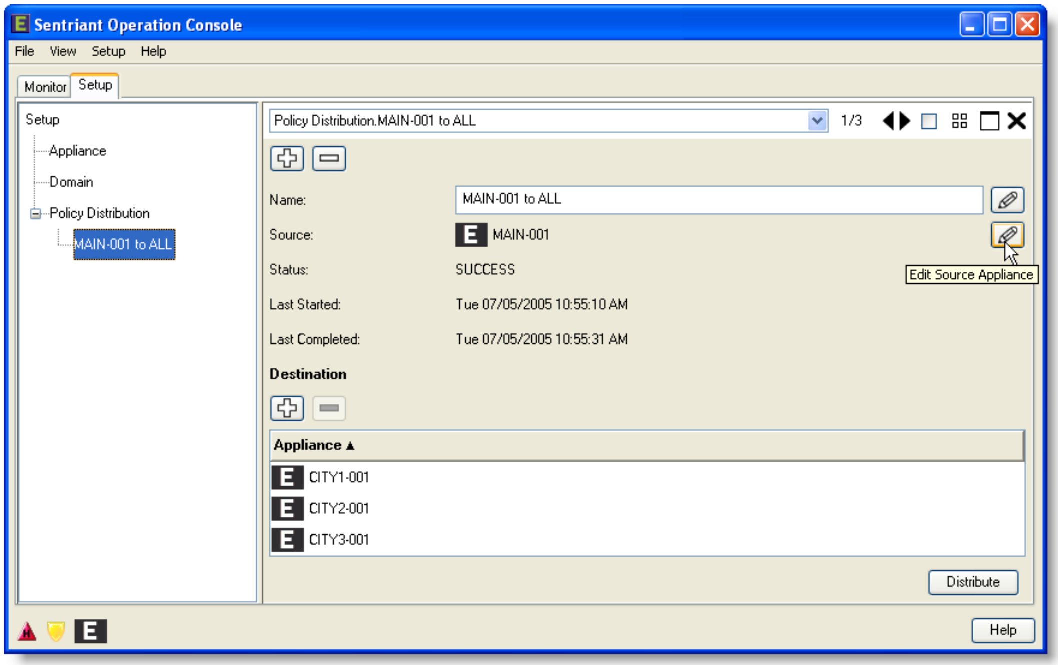
Name: MAIN to CITY CAMPUSES

Input: MAIN-001 to ALL

Appliance
CITY1-001
CITY2-001
CITY3-001

To edit the source of a policy distribution:

6 Click the **Edit Source Appliance** button.



Name: MAIN-001 to ALL

Source: MAIN-001

Status: SUCCESS

Last Started: Tue 07/05/2005 10:55:10 AM

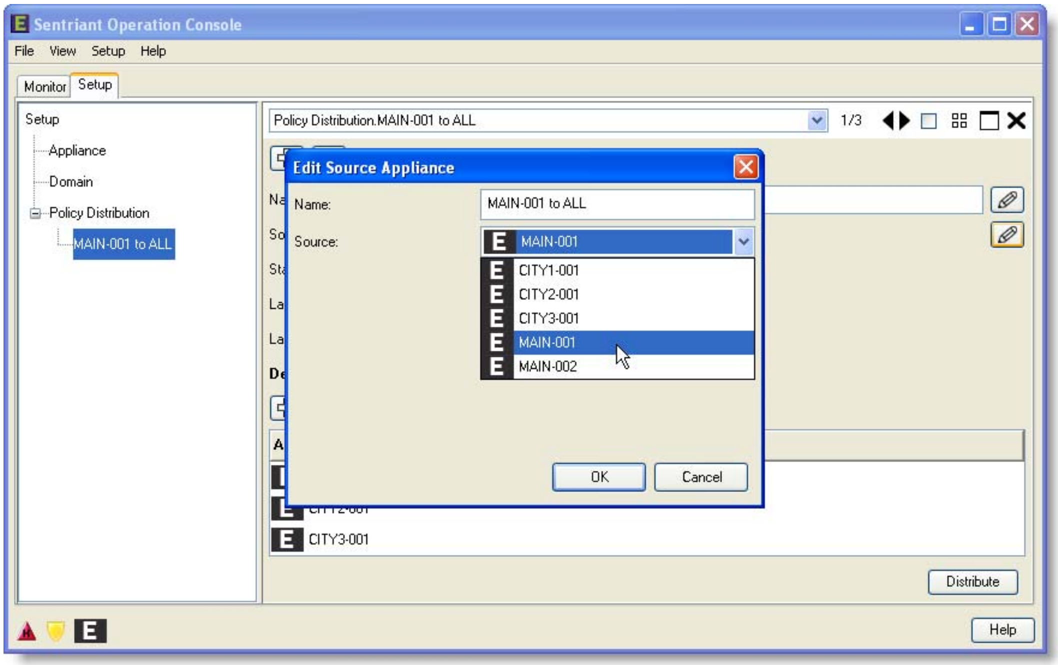
Last Completed: Tue 07/05/2005 10:55:31 AM

Destination

Appliance ▲
CITY1-001
CITY2-001
CITY3-001

7 The Edit Source Appliance dialog opens. Select an appliance from the drop-down list.

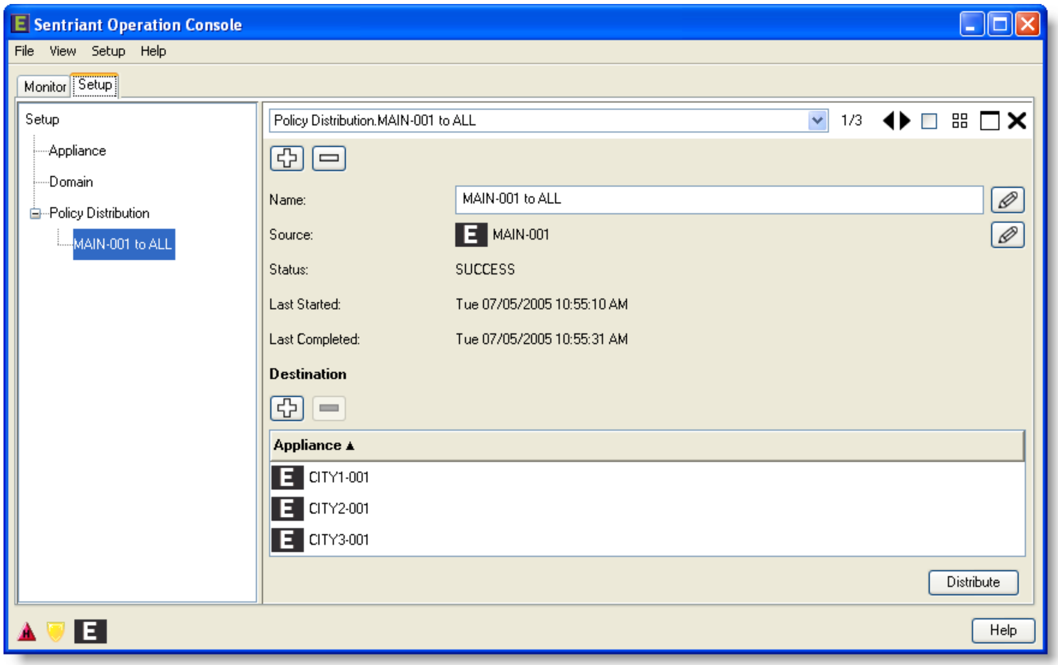
8 Click **OK**.



Name: MAIN-001 to ALL

Source: MAIN-001

The policy name and source are changed and displayed in the Information Panel.



Name: MAIN-001 to ALL

Source: MAIN-001

Status: SUCCESS

Last Started: Tue 07/05/2005 10:55:10 AM

Last Completed: Tue 07/05/2005 10:55:31 AM

Appliance ▲
CITY1-001
CITY2-001
CITY3-001

Glossary

A

access client

Workstations that have Sentriant Manager installed and that are accessing a Sentriant. Access clients, based on the type of user logged in, can perform Sentriant configuration actions, can monitor the fabric and perform manual and automatic mitigation activities.

admin

System Administrator - Extreme Networks Sentriant system user with full read/write access to system and application monitoring, display, and control commands.

alerts

The Sentriant can be configured to send alerts notifying the administrator that threat behavior has been detected. Sources or rules trigger alerts to be sent. Alerts can be sent via E-mails, SNMP SysLog, or a combination of all.

ARP Horizon

An Address Resolution Protocol (ARP) horizon is the area of a network in which MAC addresses can be resolved. ARP is also commonly referred to as Broadcast Domain or segment when referring to the Sentriant. Network devices within an ARP Horizon communicate directly without passing traffic through a router.

B

bad packet

A packet that does not conform to the protocol standard has been detected indicating a possible attack.

broadcast domain

Also known as ARP horizon, a broadcast domain is the area of a network in which all network devices can communicate with each other without going through a router.

C

cloak

A patent-pending technique by which the Sentriant unilaterally controls and terminates a communications flow between two or more computers. Cloaking can be manually or dynamically invoked by the Sentriant when threats are identified or policy conditions violated.

cloak all

Cloak All inserts itself into all communication paths that exist between all known used IP addresses of the monitored network and removes threats from the communication stream, while other traffic is allowed.

The source will remain cloaked until the configured threat time-out has been exceeded. At this time, the Sentriant removes itself from the data path between all monitored addresses and threat sources, barring the existence of another threat that would not allow uncloaking.

C (Continued)

cloak on demand

When Cloak is selected as the response to a threat, the Sentriant initially inserts itself into communication paths for only the devices that have communicated with the threat and removes the communication stream. Traffic to/from other (non-threat) hosts will be permitted. Once determined that the threat source is no longer a threat it can be Uncloaked so that communication is permitted within the Sentriant's protected segments.

communication stream

The transmission and receiving of packets between two hosts.

D

deception

A special technique that is employed by the Sentriant to mislead hackers by providing misleading data about the network. Deception uses configurable OS and IP personas to slow attackers.

decoy

A *decoy* is not a real machine on the network but rather a virtual device intended to deceive a hacker. A decoy may appear to be a functioning system but it's actually an unused IP address that does not respond to the Address Resolution Protocol (ARP) and will not transmit traffic. The Sentriant uses decoys to artificially respond to any kind of contact. The Sentriant can configure the decoy with an artificial OS personality enabling it, for example, to respond to a query or probe as a Linux, Windows 98, Windows XP-based system, or a user-customized personality.

detection

The screening and identification of network traffic for potential worms or viruses that may attack or infect hosts by the use of configurable rules. Rules are configured that look inside individual packets for suspicious behavior. If a rule is triggered, a mitigation action, or response, may be taken either automatically or manually.

dismiss

To manually dismissing a threat to a priority of watch. Threats with priority status of high, medium, low or suspect can be dismissed to a watch priority. The threat will remain a watch unless the threat triggers a rule with a higher priority level.

DNS

Domain Name System - An Internet service that translates domain names into IP addresses.

domain

A group of appliances that are administered as a unit with common rules and procedures. A domain may also have sub-domains further grouping appliances by geographical location, rules or business processes.

E

escalate

To manually escalate the priority status of a threat to a higher priority level. The priority level can be escalated from any priority to a higher priority by applying a configured rule to the threat. For example a low priority can be escalated to a high priority. The threat will remain at the higher priority until the rule times out. The threat, if still present, will return as the lower priority if it triggers a rule.

E (Continued)

event viewer

The event viewer panel used to view and manage network activity events. The Events Viewer maintains logs about Sentriant, configuration, network activity events.

exclude

Exclude is used to fine tune IP Addresses and ports to be monitored when Include is used to monitor range(s) of IP Addresses. For example, if an IP Address falls within the Include IP Addresses that are used for network management purposes only, it may become necessary to exclude that IP Address to prevent erroneous threats. By adding the IP Address to the Exclude tables, it will not be monitored by the Sentriant.

F

fabric

Term used that covers the IP Addresses and traffic between the IP Addresses monitored by Sentriant(s). A fabric may be made up of multiple switches, gateways, and Sentriants of a WAN.

I

include

Include allows the configuration of specific IP Addresses and ports to be monitored by the Sentriant. IP Addresses and ports are added to a rule using a session profile that sets a single or range of source and/or IP Addresses and ports. When session profiles are added to a rule, only values that are in the session profile are monitored on the source segment. For example, if you wish to create a Too Many Protected Web Server rule where protected web server IP addresses are 10.10.10.1 thru 10.10.10.5 with one more at 10.10.10.19, then a session profile would have the following values:

Source IP - empty

Source Port - empty

Target IP - 10.10.10.1-5,19

Target Port - empty

If you only wanted to count the threats on port 80, then you would change the Target port to 80.

If no session profiles are entered, then by default all traffic will be included.

IP Address

Also referred to as Internet protocol address. It consists of four 8-bit numbers (represented as integers) called octets. Most often, each part of the IP address is a number between 0 and 225; however, the first number must be less than 224 and the last number cannot be 0. Networks using the TCP/IP protocol to route messages based on the IP address of the destination. Connecting a private network to the Internet requires using registered IP addresses (called Internet addresses) to avoid duplicates.

M

MAC Address

The low-level address consisting of a 48-bit hexadecimal number (12 characters) assigned to a device on an ethernet network. MAC addresses are translated to IP addresses via ARP. Each NIC is assigned a unique address at the factory.

MAC Validation

A process performed by the Sentriant that validates the low-level address sent by a host consisting of a 48-bit hexadecimal number (12 characters) assigned to a device on an ethernet. MAC Addresses are translated to IP addresses via ARP. Each NIC is assigned a unique address at the factory. In cases where MAC Addresses are found to be spoofed as, the Sentriant will trigger a rule that may either cloak, snare, or send decoy information based on the rule that is triggered.

management segment

The segment identified during Sentriant configuration that will be used to manage and monitor.

manual escalation

The Sentriant admin has chosen to manually respond to a specific source IP Address as a potential threat and change the threat priority to high, medium or low which will trigger a rule and configured mitigation actions.

masked source

When a threat is detected by the Sentriant but the source of the attack cannot be immediately determined, the source is referred to as masked. This usually occurs during initial network segment startup when the Sentriant has not yet *learned* all of the address mappings, or when a spoofed packet is sent through a gateway utilizing a protected IP Address.

monitor

The ability to detect and track suspicious and potentially threatening network behavior across one or more network segments that are under the protection of the Sentriant. Threat behavior can be monitored whether it originates from a source inside or outside of the Sentriant's protected range.

N

native segment

The portion of an ARP Horizon or Broadcast Domain that is native to a switch and does not need Qtag identifiers since the IP Addresses are not broadcast as a VLAN.

network segment

The portion of an ARP Horizon or Broadcast Domain that is protected by the Sentriant. The segment has multiple attributes that are necessary for proper operation that are configured using the Edit Configuration for segments.

NMAP

A network scanning/mapping tool used to determine the network topology and type of network.

NTP

Network Time Protocol. A standard for synchronizing your system clock with the “true time” defined as the average of many high-accuracy clocks around the world.

O

observer Extreme Networks Sentriant system user with read-only access to the system and application controls.

operator Extreme Networks Sentriant system user with read/write access to all of the application monitoring and display commands but does not have access to network segment configuration and Sentriant maintenance.

P

packet A piece of a message transmitted over a network. One of the key features of a packet is that it contains the destination address in addition to the data.

packet match An Sentriant can be configured with packet match rules. The administrator can define a specific portion of the packet which must match a supplied data value. In defining the packet location, the admin must specify the packet base. The base is a well known, defined location in the packet (by protocol specification).

- **application** A packet match rule specifying an application-based location indicates that the offset and data parameters should be applied starting at the end of the the Transport Header. This is typically considered the data portion of the TCP or UDP packet. In ICMP it marks the end of the ICMP control header and the beginning of the ICMP data. The application header extends to the end of the data packet.

- **data/mask** A packet match rule that compares the contents or data of a packet (at the specified base/offset) with the user supplied data value. If a mask is specified, then the contents of the packet (at the specified base/offset) will first be logically AND'ed with the Mask value and the result will be compared to the data value.

- **frame** A packet match rule specifying a frame-based location indicates that the offset and data parameters should be applied starting from the Frame header of the packet. Most commonly, the Ethernet header is stored within the Network portion of the packet.

- **match** An administrator can configure whether packet match rules should trigger for packets that Match the defined parameters, or for packets that do not match the supplied parameters.

- **network** A Packet Match rule specifying a network-based location indicates that the offset and data parameters should be applied starting from the Network header of the packet. Most commonly, the IP protocol header is stored within the Network portion of the packet.

P (Continued)

offset

For packet match rules, the administrator must first define a base from which an offset can be defined. This will describe the network header that should be inspected. The offset defines the number of bytes, into a specified header, that should be advanced before inspection begins.

The offset value also provides a second field for input (after a '-'). If this field is populated, the Sentriant will search the data packet, starting at the specified offset and end at the value provided in the second input field.

receive

The admin can specify the direction in which packet match traffic should be inspected. If Receive is selected, then packets which are received by the source (as responses to a communication stream initiated by the source) are inspected to determine if the packet contents match the supplied parameters.

transmit

The admin can specify the direction in which packet match traffic should be inspected. When Transmit is selected, the packets which are transmitted by the source are inspected to determine if the packet contents match the supplied parameters.

transport

A packet match rule specifying a transport-based location indicates that the offset and data parameters should be applied starting from the Transport header of the packet. Most commonly, the TCP, UDP or ICMP protocol header is stored within the Transport portion of the packet.

personality

A personality is configured artificial OS personality that is used to mislead source hosts when a query or probe is conducted. A personality can be configured as a Linux, Windows 98, Windows XP-based system, or a user-customized personality. Responses to hosts can be set to snare, slow scan or both. Ports may be added to the personality that are watched for source host activity.

personality set

A personality set is made up of multiple personalities. The percentage of personalities sent to a host may be configured within a set. For example, a personality set may consist of Linux, Windows 98, and Windows XP. Each is set to 30 percent as a response with the remaining 10 percent set to vacant.

ping flood

A ping flood is an attempt to use Internet Control Message Protocol (ICMP)-based packets, (for example, to attempt a denial of service ping attack) to determine the layout of a network.

policy

A collection of configuration settings that are applied to a segment set that defines Sentriant detection and response actions.

port scan

In a port scan, a host on the network scans a specified number of ports on a single target has been detected. This could indicate an attempt to determine what services are running on the scanned host.

primary

Refers to the primary Sentriant that is managing a fabric. The primary Sentriant is configured with the management segment, database and has support logs for the fabric.

P (Continued)

protected range

The range of IP Addresses under the protection of an Sentriant.

Q

Qtag

The Institute of Electrical and Electronics Engineers (IEEE) standard 802.1Q enables VLAN traffic to span many broadcast domains or switches. It does this by inserting a special *Qtag* that carries a VLAN identifier (VID) into each Ethernet frame. This *tagged* traffic carries VLAN membership information between switches, thus enabling a VLAN to span multiple switches.

R

radial view

Displays the entire enterprise deployment graphically like the spokes of a wheel. The center of the wheel is the highest domain level. Each spoke represents a branch of the network. Appliances are located at the end of each branch.

response

The action taken by the Sentriant, using configurable rules, to counter potential worms or viruses that may attack or infect hosts. Rules are configured that look inside individual packets for suspicious behavior. If a rule is triggered, a mitigation action, or response, may be taken either automatically or manually.

rollback

The act of applying a previously saved configuration policy to a Sentriant appliance.

rule

Rules are what drive the detection and response actions of the Sentriant. Once a segment is configured and is being monitored by the Sentriant, configurable rules are created to detect and respond to malicious network activity.

rule set

A collection of rules assigned to a segment set.

S

segment set

A Segment Set is a collection of segments that exhibit similar policy behaviors. For example, if a Segment Set is reserved for DHCP clients (laptops), then a set can be created containing all laptops within a segment and then parameters can be set for rules, deception distributions and modifiers. Creating segments is accomplished using the Segment Assistant.

slow scanning

A tactic employed by the Sentriant specifically designed to significantly increase the time it takes for an external host to scan the monitored network, causing the attacker to consume time and resources. This feature is only enabled when deception is turned on and slow scan is part of a configured personality.

SMTP

Simple Mail Transport Protocol - A TCP-based application layer, Internet standard protocol for sending e-mail messages between servers. The Sentriant uses it to send alerts and allows remote monitoring.

S (Continued)

SOC Acronym for Sentriant Operation Console.

snaring A Sentriant uses a special technique to engage and hold TCP-based attacks, thus preventing them from spreading. Snaring ties up an attack thread so it cannot move to another computer, slowing or even stopping the attack. This feature is enabled when deception is turned on and if snaring is part of a configured personality.

SNMP *Simple Network Management Protocol* - Industry standard network management protocol that is used to send alerts.

source An IP Address that has originated traffic in a monitored network segment and attempts to communicate with a target.

SPAN port *Switched Port Analyzer* - Mirrors network traffic from a switched segment onto a specified port for traffic monitoring purposes.

spoof count The number of spoof IP addresses sent from a computer or device. For example, a source IP Address of 1.1.1.2 has spoofed IP Addresses of 2.2.2.1, 2.2.2.2, 2.2.2.3 and 2.2.2.4 totalling four(4).

spoof origin The computer or location where a spoofed as IP Address or spoof packet originated. In IP spoofing, an attacker gains unauthorized access to a computer or a network by making it appear that a malicious message has come from a known computer by "spoofing" the IP address of that machine.

spoof packet A packet whose source IP has been changed but its MAC address remains constant.

spoof packets Packets that are sent out from the local network but have a false source address. This could signal the presence of a virus, worm or a rogue gateway.

spoofed as The address that was given as the false source of a spoof packet.

sub-domain A domain with a domain.

suspect A suspect is a configurable priority level within the Sentriant. Any configured rule can escalate a threat to a suspect level.

SysLog A method of collecting message logs from many systems. Each system sends short text messages to a syslog recorder. The recording system may record these in any desired manner including writing them to a file, sending them on to other systems, and printing them out. The Sentriant Manager uses SysLog for alerting users of activities on Sentriants.

T

target The host or workstation that a source host attempts to communicate with.

T (Continued)

too many externals
A local system on the network is contacting a large number of external hosts. This could signal the presence of a virus or worm.

too many unprotected
A local system on the network is contacting a large number of remote hosts. This could signal the presence of a virus or worm.

too many used
Too many used (i.e.,*real*) IP addresses have been contacted by a single host. A used address is an address that has a real machine associated with it.

too many unused
The Sentriant has detected a source attempting to contact too many unused IP Addresses.

U

Universal Time
A time scale that is the basis for the worldwide system of civil time. Referred to as *Coordinated Universal Time* (abbreviated UTC), this time scale is maintained by highly precise atomic clocks located around the world. UTC is accurate to a nanosecond per day.

used
A host or workstation using an IP Address within the protected range of a Sentriant. It responds to Address Resolution Protocol (ARP) requests and sends traffic on the network.

V

VLAN
Virtual Local Area Network - A *logical*, or *administratively configured*, LAN or broadcast domain that is defined by software rather than by fixed, physical port connections.

W

watch
A watch is a source that has communicated within (or itself resides within) the protected range(s) of the Sentriant.

Index